Securepoint Personal Firewall & VPN Client

Version 3.6

Table of contents

Introduction....3
1 General information on the Securepoint Personal Firewall....4
1.1 Technical features....4
1.2 System requirements....4
1.3 Service and Support....5
2 Installation and registration of the Securepoint Personal Firewall....6
2.1 Installation....6
2.2 Registration....10
2.2.1 Registration....10
3 General information on the Securepoint Personal Firewall....12
3.1 Starting the Securepoint Personal Firewall....12
3.2 Securepoint Firewall Symbol in the Windows task bar....13
4 Overview of the main window of the Securepoint Personal Firewall....14
5 Administrating the Securepoint Personal Firewall....16
5.1 General settings....16
5.1.1 General settings....16
5.1.2 Alarm notification....18
5.1.3 Log & Advance....19
5.2 Configuraing rules....20
5.2.1 Application tries to communicate....21
5.2.2 Overview of applications....22
5.2.2.1 Add application....24
5.2.2.2 Change application....25
5.2.2.3 Delete application....27
5.2.3 Viewing rules....28
5.2.3.1 Defining and changing firewall rules....30
5.2.3.2 Deleting firewall rules....31
5.2.3.3 Library of firewall rules....32
5.3 VPN....34
5.3.1Authentification procedure....35
5.3.2 To set up a pre-shared key....36
5.3.3 To set up an X.509 certificate....37
5.3.4 To set up, edit and delete VPN connections....39
5.3.4 To configure a VPN connection....40
5.4 A VPN with Securepoint Firewall & VPN Server and X509 authentication....42
5.4.1 Creating the firewall rules for IPSec connections....43
5.4.2 Creating X509 certificates....51
5.4.3 Configuring the IPSec connection on the firewall....56
6 Recording and reporting with the Securepoint Personal Firewall....62
6.1 Viewing record....62
6.2 Overview of statistic....65
7 Update....66
8 Uninstall the Securepoint Personal Firewall....67
Glossary....68
General questions and answers concerning security....72
Questions and answers to the Securepoint Personal Firewall....77

Introduction

Why do you need a firewall?

The job of your Securepoint Personal Firewall is to protect your PC from unwelcome access from the outside and to protect your personal data thereby. Protecting the PC from attacks from the internet is the most important field of application today. The Securepoint Personal Firewall represents the intersection between your local PC and the internet. It also supervises all transfer of data. The Securepoint Personal Firewall automatically hides your PC in the internet. That means it makes the PC invisible for possible attackers and catches suspicious connections. Unnoticed passing-on of personal data will become impossible.

Basics concerning the security strategy of the Securepoint Personal Firewall

The basic security strategy for you consists of several elements and can be formulated by the following statements:

- Without permission, everything is forbidden
  The basic setting of the Securepoint Personal Firewall only allows those applications whose communications were explicitly permitted.

- Minimal rights of access
  Each program on your PC should only own those right of access which it actually needs. The Securepoint Personal Firewall supports you in this and recognises automatically which programs are tending to communicate with the exterior. You will be asked if you want to allow this program to communicate or if you refuse to give your allowance. Thereby, the working surface which could possibly be attacked is essentially reduced.

- Easy control and overview
  An easy control and overview allows you to concentrate on fundamental settings.

- Lines of defence in several layers
  Do not rely on a single system of defence. In any case, use other security systems such as virus scanners in addition to the Securepoint Personal Firewall. Since the Securepoint Personal Firewall is compatible with virus scanners, e.g. of AntiVir, you can additionally operate with a virus scanner.

1 General information on the Securepoint Personal Firewall

1.1 Technical features

Languages:	German, English
Features relevant for security:	Kernel mode driver for seamless integration in the operating system
	Supporting all IP protocols (TCP, UDP, IP, ICMP, ESP, GRE etc.)
	Recognising of connections and applications of rules based on firewall
	Wizard for firewall rules
	Protection of password for changing rules and settings
	Emergency Lock – blocking of all connections
	Packet Filtering Engine
	Stateful Packet Integrity Check Engine
Surface:	State-Of-The-Art working surface in windows design
Recording:	Recording per day
	Recording per process
	Record shown in report of incidents of windows
Updates:	Automatic quest for updates integrated in application

1.2 System requirements

Operating system:	Windows 2000 Professional
	Windows XP Home
	Windows XP Professional
	Windows Server 2003 / .NET-platform
Hardware:	Processor: 86x-compatible processor with at least 300MHz
	At least 64 MB RAM
	3MB hard disk store

1.3 Service and Support

In case you have questions to the Securepoint Personal Firewall & VPN Client, you can contact the online forum.

- http://www.pcschutz.de/forum

For further questions you can also email the Securepoint Support:

- support-pcschutz@securepoint.de

You find further information on new software/updates and news on the Securepoint Personal Firewall under:

- http://www.securepoint.cc/

2 Installation and registration of the Securepoint Personal Firewall

2.1 Installation

Prior to installing the Securepoint Personal Firewall

Please note:

- Due to security reasons and to avoid a possible impairment, close all opened applications on your PC.
- Close your anti virus product to ensure a safe installation.
- Due to security reasons and to avoid conflicts, uninstall other firewall products.

Installation of the Securepoint Personal Firewall

Proceed as follows in case you have a CD-ROM at hand:

- To install from the CD-ROM, put it in the CD-ROM driver of your computer.
- Click on the installation file to start the Setup Wizard (Fig. Setup Wizard - start).

Proceed as follows in case the program is directly at hand (for instance by downloading):

- Double click on the installation file to start the Setup Wizard (Fig. Setup Wizard - start).

Just follow the instructions of the set-up assistant. It will save guide you through the installation of the Securepoint Personal Firewall.

Setup - Securepoint Personal Firewall & VPN Client
Welcome to the Securepoint Personal Firewall & VPN Client Setup Wizard
This will install Securepoint Personal Firewall & VPN Client Version 3.6.3 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
SECUREPOINT
PERSONAL FIREWALL & VPN
Next >
Cancel

Fig. Setup Wizard - start

- Click on the button *Next* in case you would like to go on with the installation.

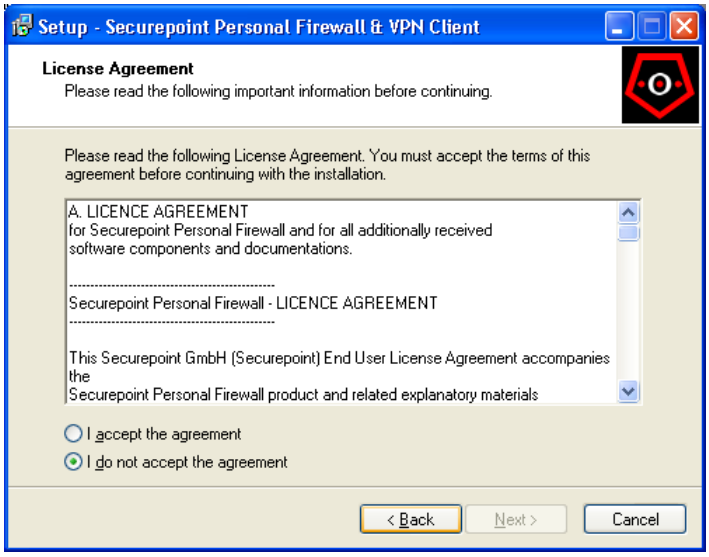

Setup - Securepoint Personal Firewall & VPN Client
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
A. LICENCE AGREEMENT
for Securepoint Personal Firewall and for all additionally received software components and documentations.
Securepoint Personal Firewall - LICENCE AGREEMENT
This Securepoint GmbH (Securepoint) End User License Agreement accompanies the
Securepoint Personal Firewall product and related explanatory materials
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel

Fig. Setup Wizard – License Agreement

- Read the license agreement..
- Click on *I accept the agreement* to go on with the installation.
- Click on the button *Next*.

- In case you do not agree with the licence agreement, click on *I do not accept the agreement*. In this case, you will not be able to go on with the installation.

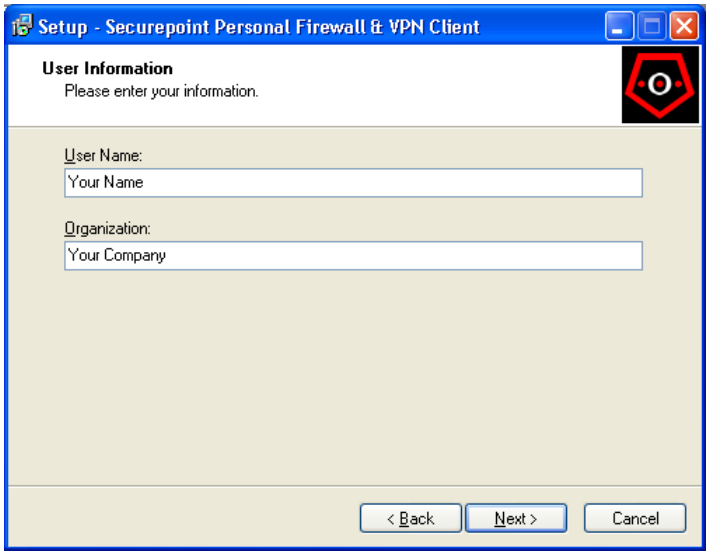


Fig. Setup Wizard – User Information

- In the fields *User Name* and *Organization*, fill in your personal user's data.
- Click on the button *Next*.

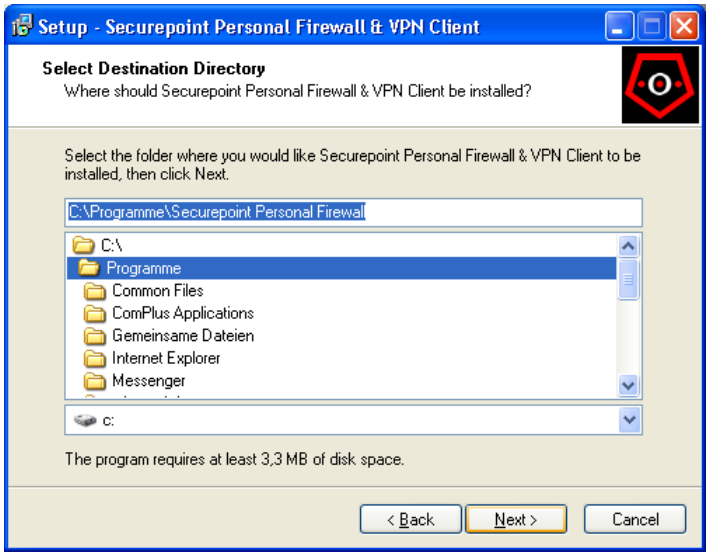

Setup - Securepoint Personal Firewall & VPN Client
Select Destination Directory
Where should Securepoint Personal Firewall & VPN Client be installed?
Select the folder where you would like Securepoint Personal Firewall & VPN Client to be installed, then click Next.
C:\Programme\Securepoint Personal Firewall
C:\
Programme
Common Files
ComPlus Applications
Gemeinsame Dateien
Internet Explorer
Messenger
c:
The program requires at least 3,3 MB of disk space.
< Back
Next >
Cancel

Fig. Setup Wizard – Destination Directory

- Select the folder in which you would like to install the Securepoint Personal Firewall. According to the standard, the program will be saved in your folder *Program Files*.
- Click on the button *Next*.

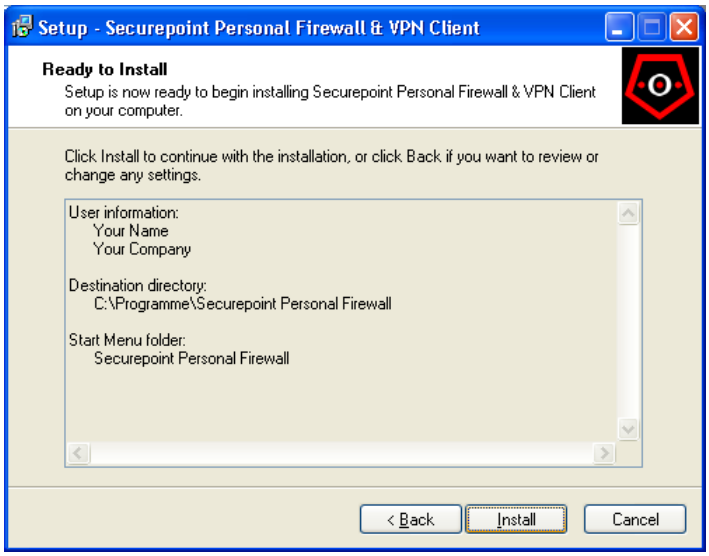

Setup - Securepoint Personal Firewall & VPN Client
Ready to Install
Setup is now ready to begin installing Securepoint Personal Firewall & VPN Client on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
User information:
Your Name
Your Company
Destination directory:
C:\Programme\Securepoint Personal Firewall
Start Menu folder:
Securepoint Personal Firewall
< Back
Install
Cancel

Fig. Setup Wizard – Ready to Install

- Click on the button *Install* to start with the installation.
- Click on the button *Back* to change or check your settings.

The progress of the process of installation will be shown. The process does usually only take a few seconds, but can take more time depending on the system.

Setup - Securepoint Personal Firewall & VPN Client
Completing the Securepoint Personal Firewall & VPN Client Setup Wizard
To complete the installation of Securepoint Personal Firewall & VPN Client, Setup must restart your computer. Would you like to restart now?
Yes, restart the computer now
No, I will restart the computer later
SECUREPOINT
PERSONAL FIREWALL & VPN
Finish

Fig. Setup Wizard - End

To finish the installation the Securepoint Personal Firewall, the Setup Wizard has to restart your computer. **Your computer will only be protected after restarting !**

- Click on *Yes, restart the computer now* to restart your computer immediately.
- Click on *No, I will restart the computer later* to restart your computer sometime later.
- Click on the button *Finish*.

After successful installing the Securepoint Personal Firewall and re-starting the computer, the Securepoint Personal Firewall is available and ready for usage.

2.2 Registration

After installing, that means before firstly using the Securepoint Personal Firewall, the Register Wizard will automatically be opened. (*Fig. Register Wizard*).

2.2.1 Registration

Securepoint Personal Firewall
SECUREPOINT
PERSONAL FIREWALL & VPN
Welcome to Securepoint Personal Firewall
Thank you for choosing the Securepoint Personal Firewall. To get the complete access, we are asking you to register your copy.
Warning: Click here if you are using a proxy-connection.
Attention:
This program is intended to used only for PRIVATE and NON-COMMERCIAL. If you want to use this copy commercial, you have to register a commercial copy. Please contact in that case Securepoint.
Click "Next", to continue registering.
Back
Next

Fig. Register Wizard - Start

Proceed as follows in case you would like to register a test version of the Securepoint Personal Firewall:

- If your internet connection is run by the proxy, activate the respective check box (*Fig. Register Wizard*).
- Click on the button *Next*.

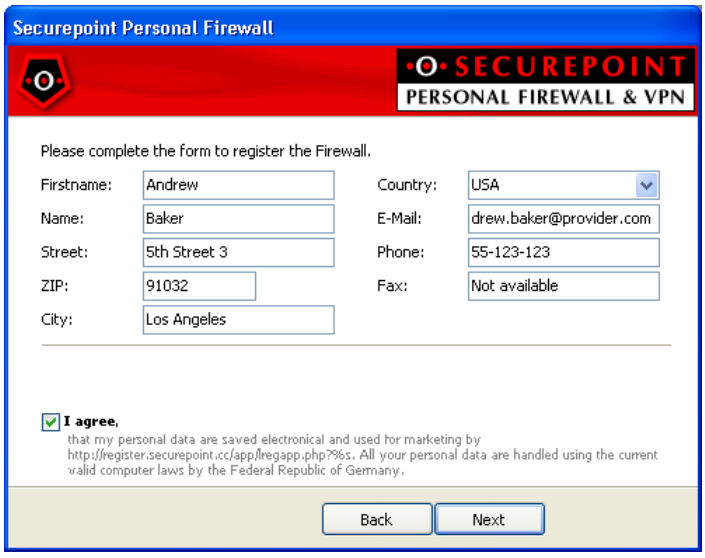

Securepoint Personal Firewall
SECUREPOINT
PERSONAL FIREWALL & VPN
Please complete the form to register the Firewall.
Firstname: Andrew
Name: Baker
Street: 5th Street 3
ZIP: 91032
City: Los Angeles
Country: USA
E-Mail: drew.baker@provider.com
Phone: 55-123-123
Fax: Not available
I agree,
that my personal data are saved electronical and used for marketing by http://register.securepoint.cc/app/lregapp.php?%s. All your personal data are handled using the current valid computer laws by the Federal Republic of Germany.
Back
Next

Fig. Register Wizard – Personal Data

- Fill in the complete user's data in the dialog.
- After inserting the complete data, click on the button *Next*.

Securepoint Personal Firewall
SECUREPOINT
PERSONAL FIREWALL & VPN
Complete
Congratulation. The firewall has been set up. You can get information in the handbook and on the Securepoint Website.
Website Securepoint: http://www.securepoint.de
Firewall handbook: Open now
Click on "Next" to close the wizard.
Back
Next

Fig. Register Wizard – Finish

- To finish the registration of your test version, click on the button *Next*.

After successful registration you have a licensed copy of the Securepoint Personal Firewall. **Note that the Securepoint Personal Firewall is free of charge used as non-commercial, private version. For comercial licensing please contact as: sales@securepoint.cc**

3 General information on the Securepoint Personal Firewall

3.1 Starting the Securepoint Personal Firewall

Your computer is automatically protected by the firewall every time you start it. You do not have to explicitly start the firewall to protect your computer.

The start screen of the firewall appears every time you re-start your computer.

Fig. Startscreen Securepoint Personal Firewall

Furthermore, the main window of the Securepoint Personal Firewall will be opened every time you re-start your computer. Via the main window, the Securepoint Personal Firewall is administered. You find information on the main window and on administering the Securepoint Personal Firewall in chapter 4.

➢ Close this window in case you do not wish any administration. The firewall will remain active in the background.

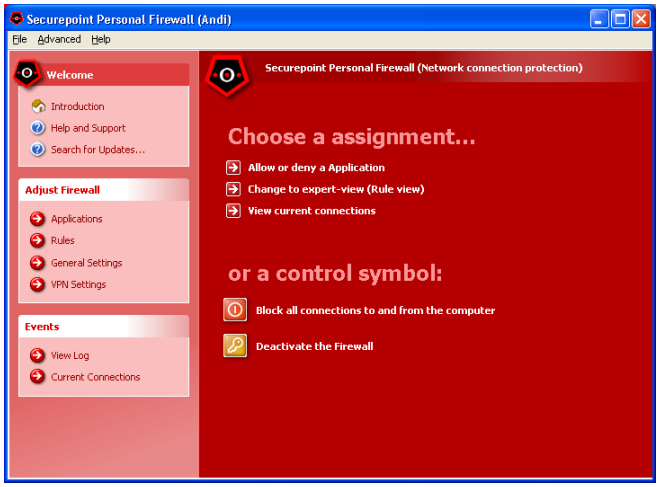


Fig. Main Window

Manually starting the Securepoint Personal Firewall via the Windows start menu

Proceed as follows in case you would like to start the Securepoint Personal Firewall manually:

➢ Click on the button *Start* in the windows task bar and select *Programs* ⇨ *Securepoint Personal Firewall* ⇨ *Securepoint Personal Firewall*.

The main window of the Securepoint Personal Firewall opens.

3.2 Securepoint Firewall Symbol in the Windows task bar

Open the main window of the Securepoint Personal Firewall via the Windows task bar

When installing the firewall, the symbol of the Securepoint Personal Firewall was added to the windows task bar. Use this symbol to open the Securepoint Personal Firewall.

- Double clicking on *Securepoint Firewall Symbol* in the windows task bar.

Fig. Securepoint Firewall Symbol in the windows task bar

The main window of the Securepoint Personal Firewall opens. You find information on the main window and administration of the Securepoint Personal Firewall in chapter 4.

Status control of the symbol of the Securepoint Personal Firewall in the windows task bar

	Securepoint Personal Firewall is active, your PC is protected
	Securepoint Personal Firewall was de-activated manually
	Securepoint Personal Firewall is inactive due to emergency
	Securepoint Personal Firewall ist inactive, settings have to be checked

Opening options of the Securepoint Personal Firewall in the Windows task bar

You can also start some basic administrations via the menu of the windows task bar without having to open the main window. .

- Click on the symbol with the right mouse key.
- Select the option at will via the shown task bar symbol.

The following options are available:

Show firewall	Opening of the main window of the Securepoint Personal Firewall
Settings	Basic settings of the firewall such as language, password, etc. (see chapter 5.1)
Add application	Adding applications (See chapter 5.2.2.1)
Add rule	Adding firewall rules (See chapter 5.2.3.1)
Emergency-off-function	All internet and network connections for communication will immediately be blocked
Help	Shows contents of help
Search for updates	Opens update assistant to search for updates and installation of the same
About...	Showing information on the firewall
End firewall	Ending the firewall, the computer will be unprotected then

4 Overview of the main window of the Securepoint Personal Firewall

After successful installation and also every time you re-start the computer, the main window of the Securepoint Personal Firewall opens automatically (*Fig. Main Window*). Via the main window, the Securepoint Personal Firewall is administered.

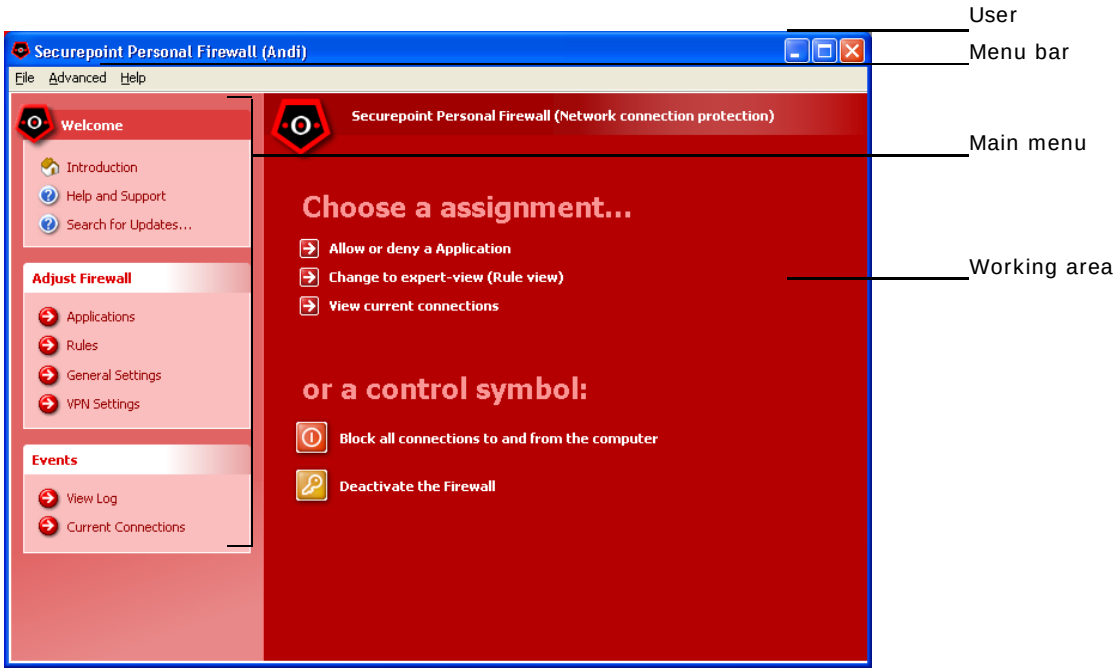


Fig. Main Window

The main window is subdivided into 4 areas:

User:	Your user's name
Menu bar:	Menu bar is subdivided into the points file and help (see menu bar main program for further explanation of these points)
Main menu:	The main menu is subdivided into the areas welcome, edit firewall, observe incidents (for further explanation of these menu points see main menu main program)
Working area:	In the working area, all selected actions are basically shown. On the starting page of the main program, you can directly select some actions via quick selection (for explanation of the available actions see actions starting page working area). Concerning present test version: notice when test version (copy) expires.

Menu bar main program

Menu points file	
Block all connections	Emergency-off function of firewall, all communication will be blocked
Deactivate firewall	Stopping of firewall, all communication will be allowed
Extended	Extended menu to administer the firewall (e.g. support)
Re-load rules	Created will be newly re-loaded on the firewall
Create support's report	Creating of a support's report to analyse errors
Settings	Basic settings of the firewall such as language, password, etc.
End firewall	Stopping of firewall, the PC will be unprotected then
Close	Closing of window of the main program, firewall is active
Menu points help	
Contents	Shows contents of help
Internet support forum	Link to support forum of the firewall
Search for updates	Opens update assistant to search for updates and for installation
Register	Opens registering assistant to register the firewall
About ...	Information on the firewall

Main menu main program

Menu area welcome	
Introduction	Introduction to the personal firewall
Help and support	Opens help and support for the personal firewall
Search for updates	Opens update assistant to search for updates and for installation
Menu area creating firewall	
applications	Opens overview of applications, what programs can do what
Rules	Opens overview of rules, explicit setting of firewall rules
General settings	Basic firewall settings such as language, password, etc.
Menu area watch incidents	
View record	Viewing record, record of applications' communication
Current connections	Overview of current connections, what happens currently

Actions starting page working area

Task	
Activate application, resp. Block them	Opens overview of applications, what programs are allowed to do what
Switch to expert's mode	Opens overview of rules, explicitly creating firewall rules
View current connections	Overview of current connections, what happens currently
Controlling Symbol	
Block connections	Emergency-off function, all communication will be blocked
Deactivate firewall	Stopping firewall, all communication will be allowed

5 Administrating the Securepoint Personal Firewall

5.1 General settings

Via the menu area *Setup Firewall*, you can make basic firewall settings.

➢ Call up of the area *Settings* via the menu area *Setup Firewall* ⇨ *General Settings.*

After that, the window settings opens (*Fig. Window General Settings*).

5.1.1 General settings

Fig. Window General Settings

Fields of input and selection	
Language:	Selection of language
Settings:	Activation of rules' management to work in area of overview of rules
Security:	Activation of password's setting
	Password: Filling in of your password
	Once more: Repetition of your password

The following *General Settings* are possible:

- Select the language at will via the choice field *Language*.

In case you activate the *Expertmode*, you are able to use the overview of rules. You find detailed information on working in the overview of rules in chapter 5.2.3.

- Activate *Expertenmodus* by ckecking the check box *Expertenanzeige aktivieren*.

You can protect the application from changing. This setting can be useful in case you would like to avoid that persons other than you, for instance your children, change configurations so that “dangerous” connections become allowed.

- Activate password setting by checking the check box *Ask Password for changes.*
- Fill in your password i the field *Password.*
- Repeat your password in the field *Repeat*.
- Save your input by clicking on the buttons *Ok*.

Asking password

In case you have activated the password function under *General Settings*, you will be asked your password every time when changing settings *(Fig. Password).*

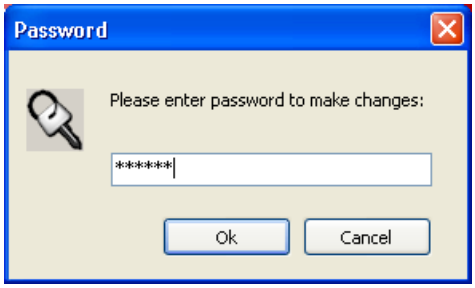


Fig. Password

You can change your password at any time under *General Settings*.

5.1.2 Alarm notification

Via activating the alarm notification, you have the possibility to play in a sound. This sound will be played in case a connection that is not allowed tries to communicate. Parallel to that, the assistant opens which will ask you for permission. You find further information on this assistant in chapter 5.2.1.

➢ Call up of he area via menu area *Setup Firewall* ⇨ *General Settings* ⇨ selection of folder *Alarm messages.*

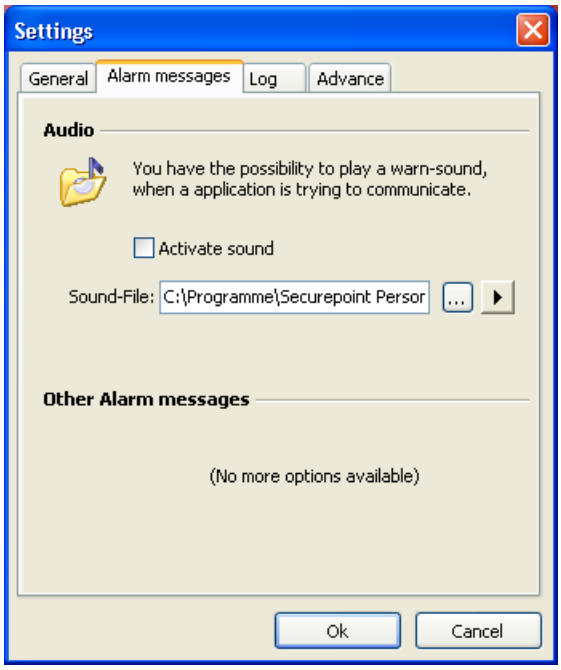


Fig. Window Settings Alarm messages

Fields of input and selection	
Sounds:	Activating playing of sounds in case of alarm notification
	Sound file: Selection of sound file
Other alarm notifications:	If you have a plugin, you can make further settings.

5.1.3 Log & Advance

➢ Call up of the area via the menu area *Setup Firewall* ⇨ *General Settings* ⇨ selection of folder *Log or Advance.*

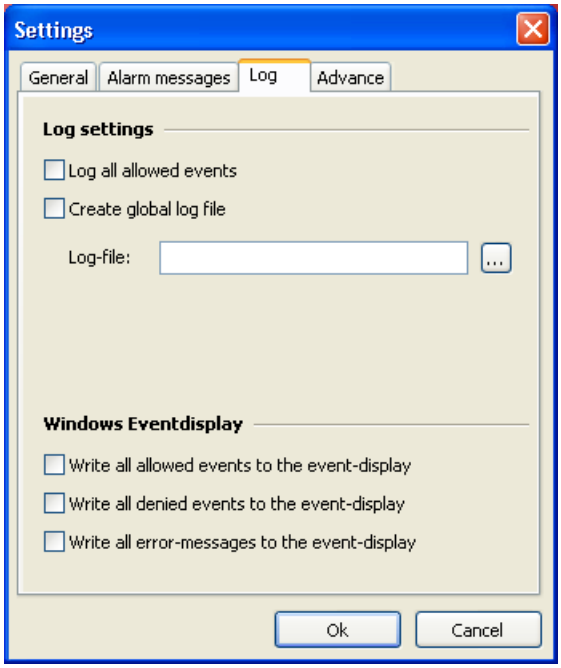


Fig. Window Log Settings

Log settings	
Log all allowed events	Normally are only non-allowed events useful for analysing. You have to activate this option if you want to log also allowed events. Please notice that the log file may get very big.
Create global file	You can specify a global log file that log all events in a seperate file.
Windows Eventdisplay	
Since Version 5.1 of Windows™ there is a system called Event Management available.	
Log:	Activate *Write all allowed/denied events* to write allowed or denied events to the Event Management.
Error:	Activate *Write all error-messages to the event-display* to write all erros to the Event Management

5.2 Configuraing rules

- **An application (program) tries to communicate, check with demand assistant:**

  By the demand assistant, you will be notified when an application (program) tries to establish a connection. You have the possibility to either allow this communication or to block it. Firewall rules will be created automatically (see chapter 5.2.1).

The firewall rules have two user's modes:

- **A mode for inexperienced users, the applications' overview:**

  You have a complete overview of all applications that are communicating with your PC in the overview of applications. Here, you can add new applications, change or delete them to allow or block them concerning communication (see chapter 5.2.2).

- **An experts' mode for experienced users, the overview of rules**

  In the overview of rules, you can explicitly define new firewall rules (see chapter 5.2.3).
  In contrast to the overview of applications, you have the possibility to define firewall rules that are to be applied to all applications due to the fact that numerous applications use the same services. Several dialogues will help you to do this as efficient and comfortable as possible. Furthermore, you have additional possibilities to make settings concerning direction, protocols, port, etc.

5.2.1 Application tries to communicate

In case you start an application (program), e.g. the Microsoft-Messenger, which tends to communicate with the outside, you will receive a notification by the demand assistant. You will thereby be notified on this communication try (*Fig. Ask window*).

In this case, the personal firewall has automatically noticed that a communication, whose application (program) has not been allowed yet, is to take place from your PC. You will be asked if you would like to allow or block the communication with this application.

Proceed as follows:

- Click on the button *Deny* in case you would like to block the application.
- Click on the button *Allow connection* in case you would like to allow the application.

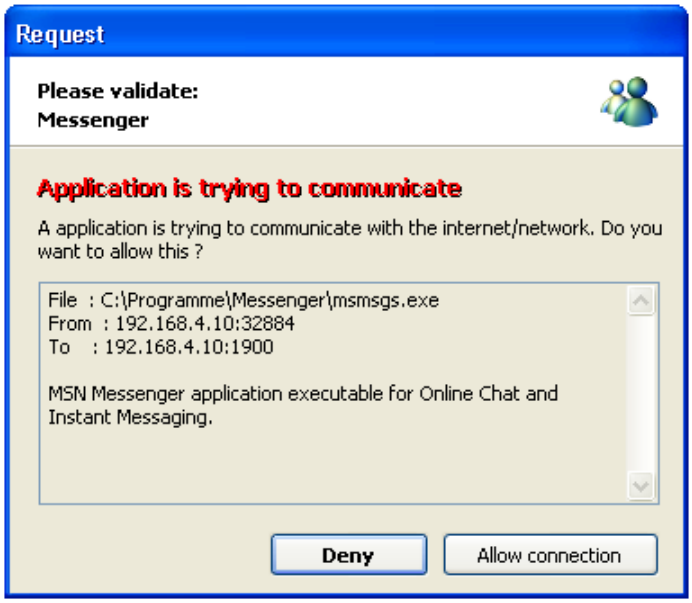

Request
Please validate:
Messenger
Application is trying to communicate
A application is trying to communicate with the internet/network. Do you want to allow this ?
File : C:\Programme\Messenger\msmsgs.exe
From : 192.168.4.10:32884
To : 192.168.4.10:1900
MSN Messenger application executable for Online Chat and Instant Messaging.
Deny
Allow connection

Fig. Ask window

Notification and buttons	
Proceedings:	Shows information on application that tries to communicate
Deny:	Block communication of application
Allow connection:	Allow communication of application

5.2.2 Overview of applications

In the overview of applications, you have the complete overview of all applications that are communicating with your PC. Here, you can add new applications, change or delete them to allow or block communication with the same.

➢ Call up of *Application-view* via menu area *Adjust Firewall ⇨ Applications.*

The window with the overview of applications opens (*Fig. Application-view*).

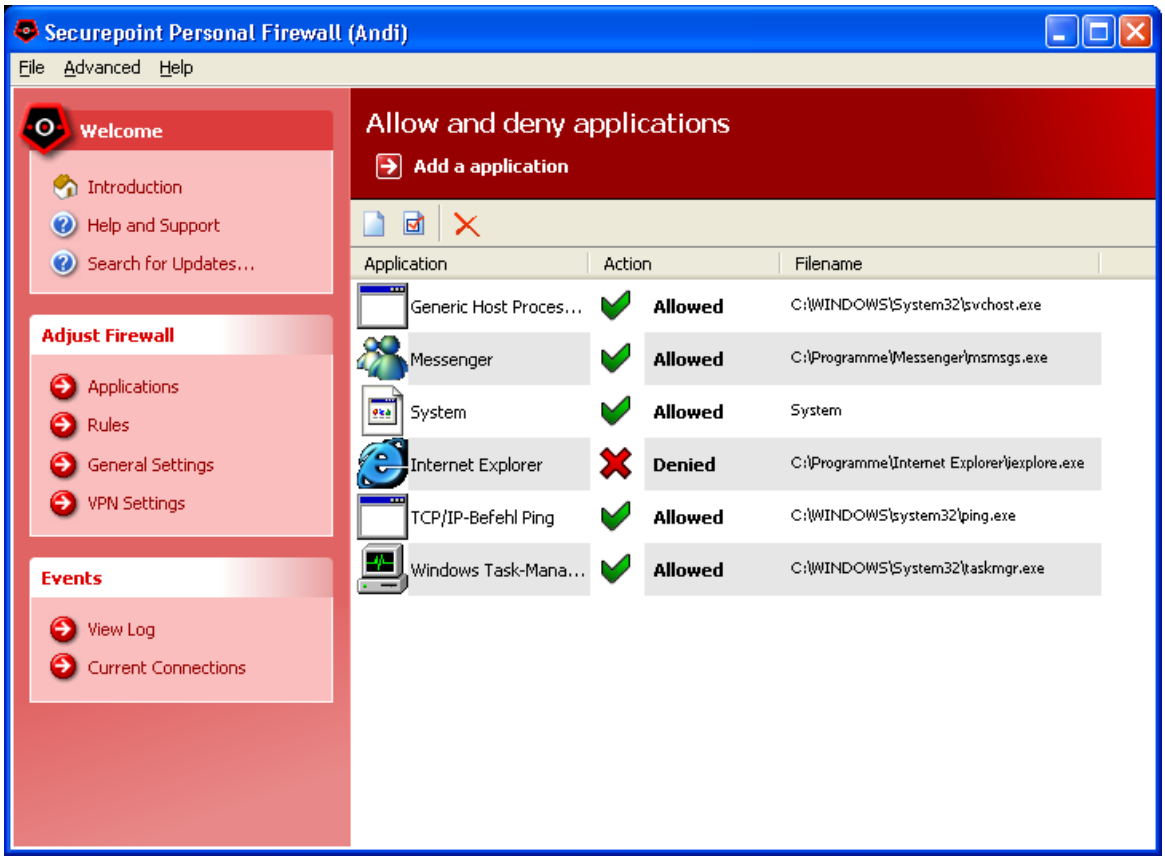


Fig. Window Application-view

Menu bar overview of applications

Fig. Menu Application-view

Icons menu bar overview of applications		
	Add:	Adding an application
	Edit:	Changing an application
	Delete:	Deleting an application

Presentation of applications

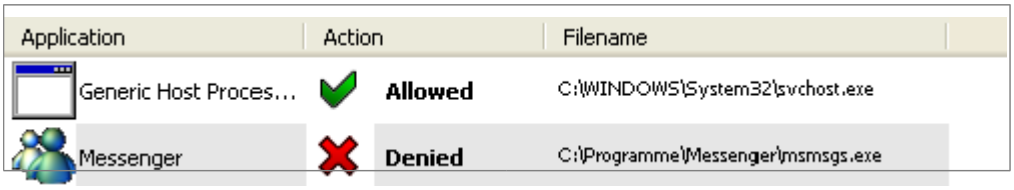


Fig. Area Applications

Presentation of applications	
Application:	Name of application
Action:	Shows if communication with the respective application is allowed or blocked
Filename:	Shows the full file and pathname of the application

5.2.2.1 Add application

Proceed as follows to add an application:

- Click on the icon *Add a application* in user's overview.
- The already familiar dialog opens in which you can select a new application (program) and open it.

The opened application will be shown in the working area of the overview of applications.

5.2.2.2 Change application

General information

Proceed as follows to change the setting of a certain application:

Click on the icon *More Information about the selected application (Edit) in the user's overview*

or

➢ Double click on an application.

After doing so, the window application will open (*Fig. Edit Application - General*).

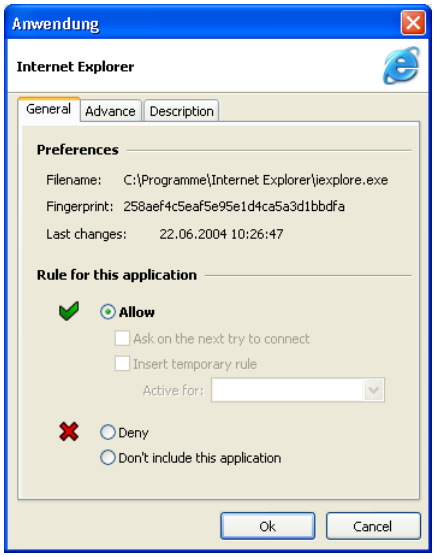


Fig. Edit Application - General

Here, you receive information on the selected applications and also change them.

Fields of input and selection	
Features	
Filename:	Shows the full file- and pathname of the application
Stamp:	Definite "finger-print" of application
Last change:	Date of last change of application
Connections of this application	
Allow:	If activating this option, the application is allowed to communicate with the outside
Deny:	If activating this option, the application is not allowed to communicate with the outside. Connections of this application will be blocked.
Do not include this application:	If activating this option, this application will not be included. This might be of interest in case you are working with firewall rules.

Extended

The *Active Process Protection* serves to discover Trojans and other programs that might gain access on other applications via DLL injection.

The firewall includes a process protection which supervises the most important windows API commands:

- CreateRemoteThread
- WriteProcessMemory
- VirtualAllocEx
- VirtualProtectEx

These functions allow users other than you to channel in any code in any current application. Numerous Trojans and viruses use this function. Therefore, the firewall observes this and automatically recognises changes in applications

➢ Select the folder *Advance* in the window *Edit Application*.

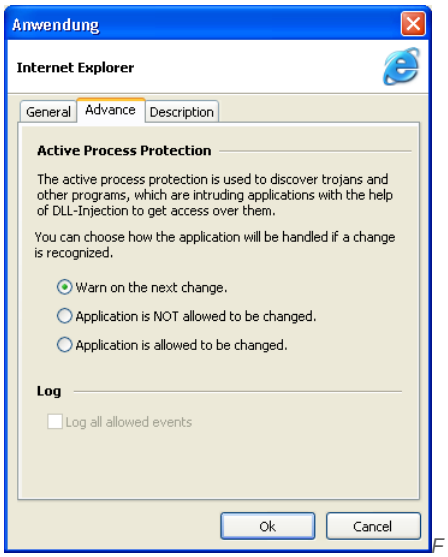

Anwendung
Internet Explorer
General
Advance
Description
Active Process Protection
The active process protection is used to discover trojans and other programs, which are intruding applications with the help of DLL-Injection to get access over them.
You can choose how the application will be handled if a change is recognized.
Warn on the next change.
Application is NOT allowed to be changed.
Application is allowed to be changed.
Log
Log all allowed events
Ok
Cancel

Fig. Edit Application – Advance

You can define how the application (program) should be treated by the firewall in case a change concerning the application has occurred.

Fields of selection	
Warn when next change occurs:	Notification by demand assistant in case another program (e.g. Trojan program) tries to change the application. This setting should remain unchanged due to security reasons.
Application is not to be changed:	The firewall will automatically block possible changes of the application.
Application can be changed:	The firewall will automatically allow changes of this application.

5.2.2.3 Delete application

Proceed as follows in case you would like to delete an application:

- Click on the application you would like to delete and thereby select it in the user's overview.
- Click on the icon *Delete Application*.

Note: The application will be deleted immediately.

5.2.3 Viewing rules

In the overview of rules, you can explicitly define and administer firewall rules. In contrast to the user's overview, you have the possibility to define firewall rules that are to be applied in general due to the fact that many applications use the same services.

Several dialogues will help you to do this as efficient and comfortable as possible. You also have further possibilities to make settings such as direction, protocols, port, etc.

Note: To be able to work with the overview of rules, you have to activate the *Expertenmodus*. In case the experts' mode in inactive, the rule assistant will be blocked.

➢ Call up of *Rules-View* via the menu *Adjust Firewall* ⇨ *Rules.*

The window of the overview of rule opens (*Fig. Window Rules-View*).

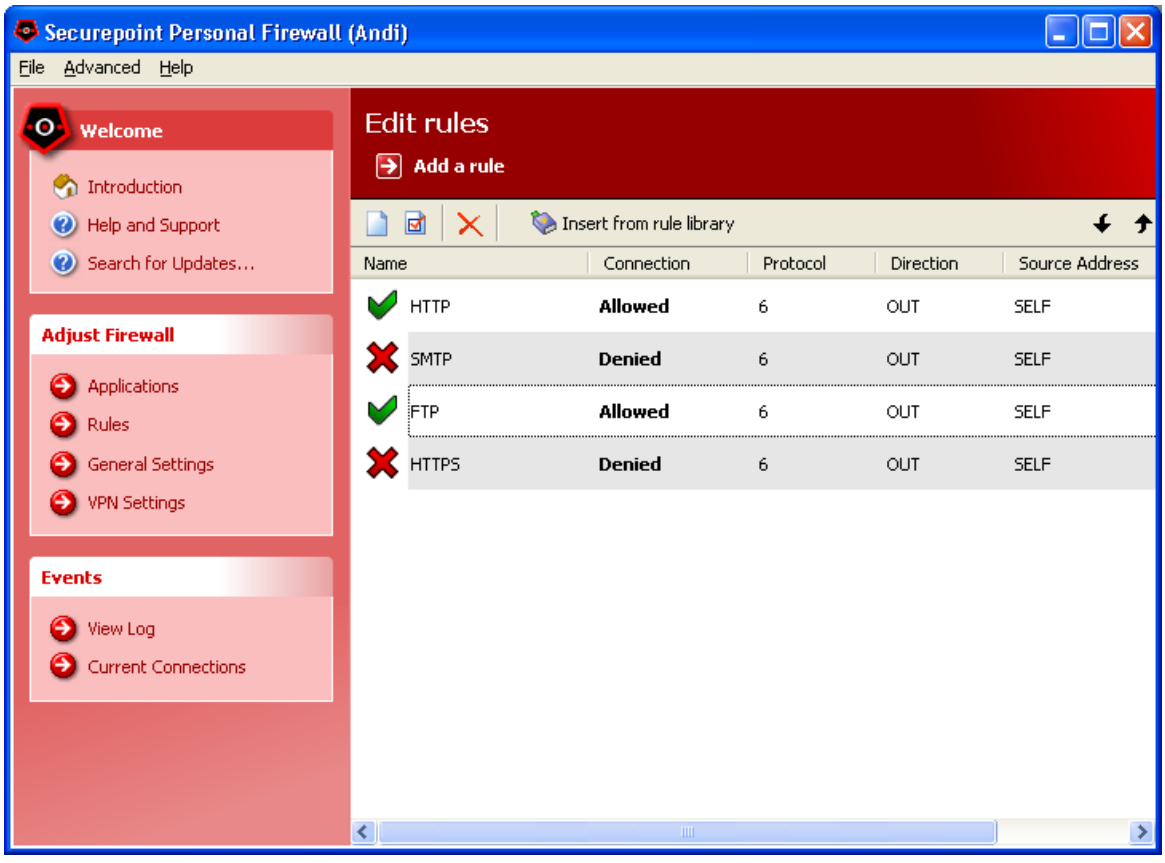


Fig. Window Rules-View

Menu bar overview of rule

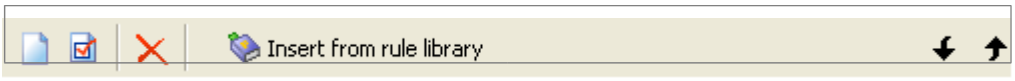


Fig. Menu Window Rules-View

Icons menu bar overview of rules	
Define rule:	Defining a new rule
Edit rule:	Changing a rule
Delete rule:	Deleting a rule
insert rule from library:	Inserting an already defined rule from the library
Rule priority downwards:	Changing of overview of rules to priority downwards
Rule priority upwards:	Changing of overview of rules to priority upwards

Presentation of rule

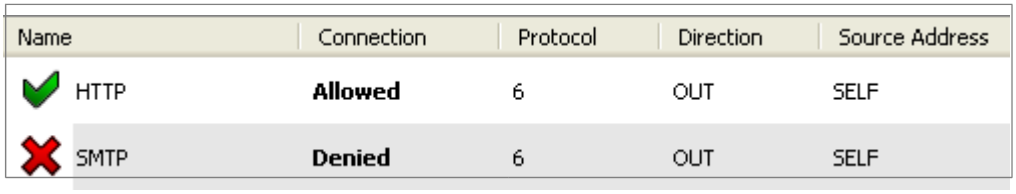


Fig. Area Rules

Darstellung Regel	
Name of rule:	Name of rule
Action:	Viewing if communication is allowed or blocked
report:	Viewing report
Direction:	Direction of the rule, entry and exit
Address of source and target:	Address of source and target of the rule

5.2.3.1 Defining and changing firewall rules

With the help of the rules' editor, you can quickly and easily define new firewall rules.

Proceed as follows:

- Click on the icon *Add.*

The window rules with the rule editor opens (*Fig. Rules-Editor*).

- Fill in the necessary data via the dialog window..
- Save and activate the rule by clicking on the button *Ok*.

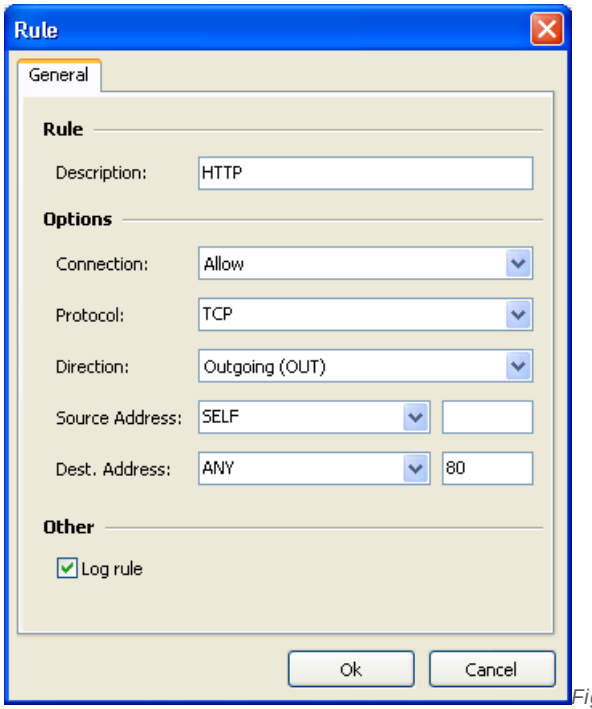


Fig. Rules-Editor

Fields of input and selection		
Name:	Name of rule	
Connection:	Selection if rule should be allowed or blocked	
Protocol:	Selection of transmitting protocol	
Direction:	Selection of direction of application	
Address of source:	Address of source of the rule	
	ANY:	All addresses (0.0.0.0)
	SELF:	Some addresses viewed from the outside
	LOCALHOST:	Local addresses (127.0.0.1)
	LOCALNET:	Local network
Address of target:	Address of target of the rule	
Record:	By activating, the connection will be recorded	

5.2.3.2 Deleting firewall rules

Proceed as follows in case you would like to delete a firewall rule:

- Click on the rule you would like to delete and thereby select it the in the overview of rules.
- Click on the icon *Delete Rule*.

Attention: The rule will be deleted and deactivated immediately.

5.2.3.3 Library of firewall rules

You further have the possibility to insert pre-defined rules from the already existing library. This makes it easier for you to get familiar with and to learn how to create firewall rules.

➢ Click on the icon *Insert from Library*.

After that, the window library opens (*Fig. Window Library*).

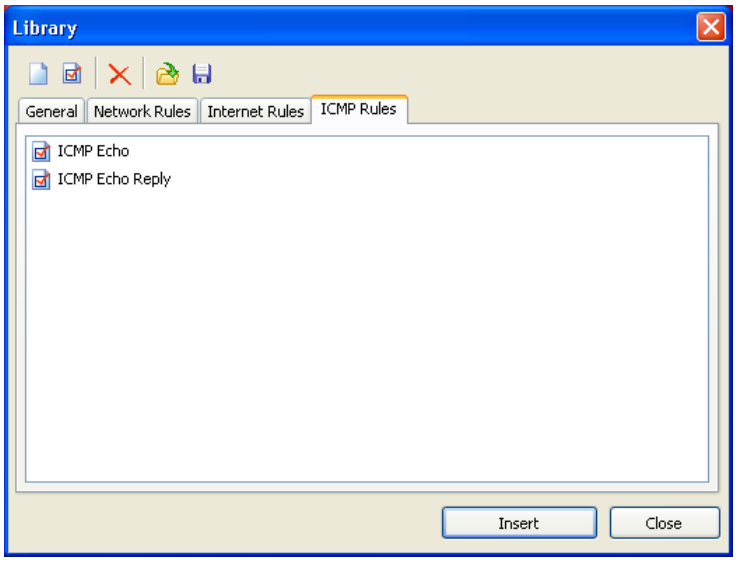


Fig. Window Library

Menu bar library		
	Define rule:	Defining of a new rule
	Edit rule:	Changing a rule
	Delete rule:	Deleting a rule
	Import rule:	Importing an already existing rule
	Export rule:	Exporting an already existing rule

To provide for a better overview, the library contains pre-defined categories in which the several rule are put. The categories can be extended or changed when creating new rules.
Categories of library of rules:

- General
- Network rules
- Internet rules
- ICMP rule

Inserting a rule from the library

- Double clicking on the selected rule

or

- Single clicking on the selected rule and click on button *Insert*.

Defining of a new rule for the library

- Select the category in which the rule should be put.
- Click on the icon *Add Rule*.

You find information on how to proceed when creating a new rule in chapter 5.2.3.1.

Changing rule from the library

- Click on the rule you would like to change.
- Click on the icon *Edit Rule.*

You find information on how to proceed when changing a new rule in chapter 5.2.3.1.

Deleting a rule from the library

- Click on the rule you would like to delete.
- Click on the icon *Delete Rule*.

Note: The rule will be deleted immediately.

Importing a rule from the library

- Click on the icon *Import Rules.*
- Select the file which is to be imported.

Exporting of a rule from the library

- Click on the icon *Export Rules.*
- Fill in the file's name and save the file.

5.3 VPN

A VPN connects one or more computers or networks together, in which it uses another network, e.g. the internet, as a means of transmission. It can for example be the computer of a colleague at home or at another branch which is connected to the mainframe network via the internet.

To the user the VPN looks like a normal network connection to the target computer. The user does not see the actual transmission route. The VPN provides the user with a virtual IP connection which is tunneled through an actual IP connection.

VPN Server

In order to be able to use the Securepoint PCFirewall VPN clients and VPN programs you require a VPN server, to which you would like to set up a VPN connection. In principal this can be any VPN server. To set up the VPN use the data provided by your administrator and enter it into the Securepoint PCFirewall and VPN clients.

The data packets which are transmitted via this connection are encrypted by the Securepoint PC Firewall and VPN clients and are further encoded or decoded by the Securepoint Firewall and VPN server or by another VPN server. The Securepoint Firewall and VPN server and the Securepoint PCFirewall and VPN client use the protocol IPSec.

If you would like to set up a VPN gateway yourself, you also here receive additional examples of setting up a VPN by means of a Securepoint Firewall and VPN server and to the Securepoint PC Firewall and VPN clients.

For further information about the Securepoint Firewall and VPN server please refer to the following web site:

http://www.securepoint.cc

5.3.1 Authentification procedure

The built-in Securepoint Personal Firewall VPN support is able to support two authentification procedures:

- Pre-shared key

The pre-shared key authentification procedure is a very simple procedure which allows VPN connections to be set up quickly. For this procedure you enter an authentification phrase. This can be any character string – similar to a password. This phrase must be available for authorisation on the VPN server and to the Securepoint VPN client.

The pre-shared key procedure should not be used by the Roadwarrior connections as all Roadwarriors must use the same key.

- X.509 Certificates

X.509 certificates are a very secure way of connecting VPN servers. If you would to implement X.509 certificates you must either set up the certificates on the Securepoint Firewall and VPN servers or you must use the X.509 certificate provided by your administrator.

In order to be able to use a certificate you must first import it into the certificate administration in Windows.

5.3.2 To set up a pre-shared key

In order to set up a pre-shared key, proceed as follows:

➢ Call up the dialogue *VPN settings* via the menu *Advanced* and click on the folder *Key administraion*.

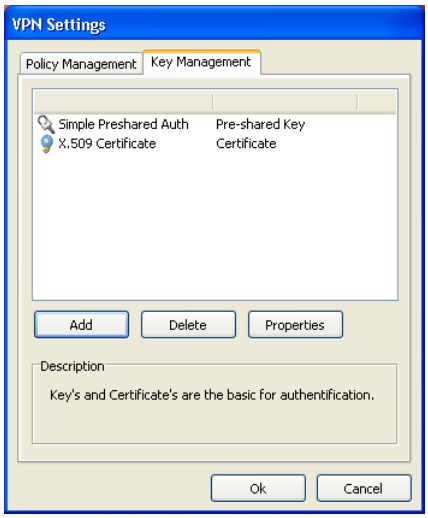


Fig. VPN settings – Key administration

➢ Click on *Add* and select *Pre-shared key*. Then the pre-shared key dialogue opens in which you can create a name for the key and set up the actual key.

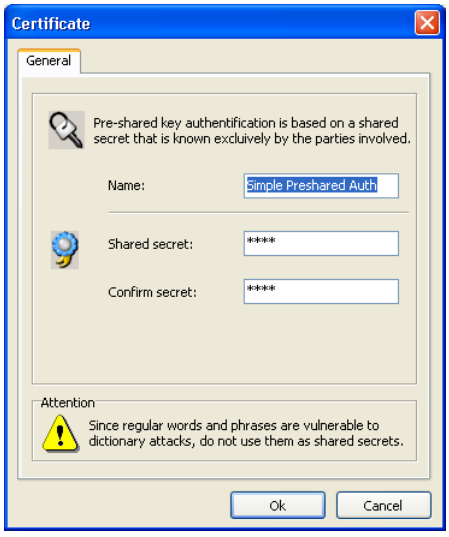


Fig. Pre-shared Key Dialogue

➢ Close the dialogue by clicking on *OK*.

You can now use this pre-shared key as an authorisation key in the rules administration.

5.3.3 To set up an X.509 certificate

In order to be able to use an certificate it must first be imported into the certificate administration in Windows. The certificate must be in PKCS #12 format (data ending: .PFX, .P12) in order to be able to be imported.

- Open the pre-configured MMC console in the Securepoint Firewall installation path in the folder VPN „ipsec.msc“.
- Click on *Certificate* and then click with the right mouse button on *Own certificates* and select *All tasks* ⇨ *Import* in order to start the import process.

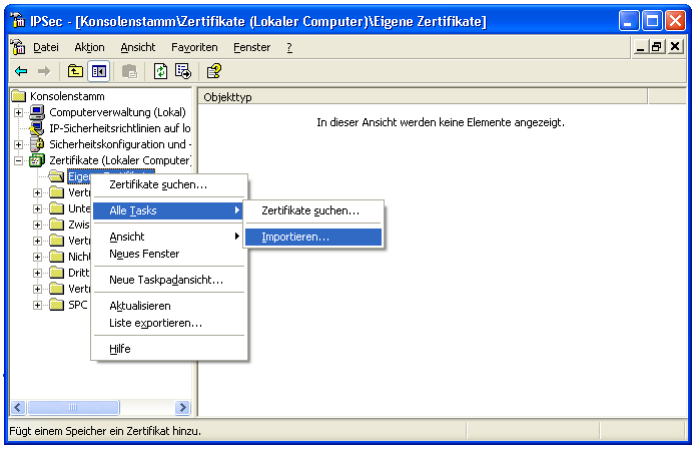


Fig. MMC console – Import certificate

- Follow the assistant and select the desired certificate.
- At the step *Save certificate* the option *Save certificate automatically* **MUST** be selected.

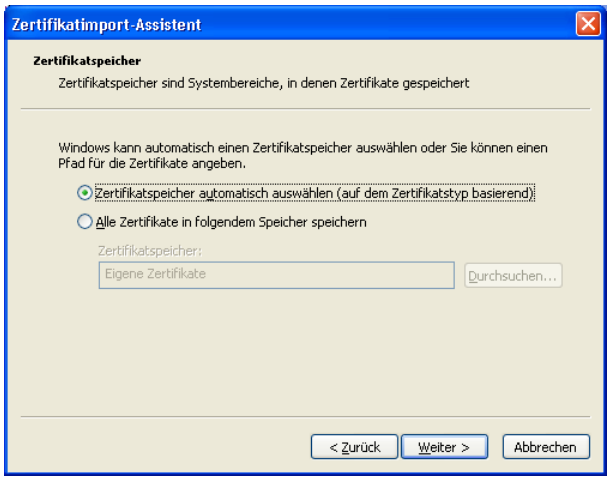

Zertifikatimport-Assistent
Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert
Windows kann automatisch einen Zertifikatspeicher auswählen oder Sie können einen Pfad für die Zertifikate angeben.
Zertifikatspeicher automatisch auswählen (auf dem Zertifikatstyp basierend)
Alle Zertifikate in folgendem Speicher speichern
Zertifikatspeicher:
Eigene Zertifikate
Durchsuchen...
< Zurück
Weiter >
Abbrechen

Fig. Certificate import assistant – Save certificate

- After the successful import you still need to name the certificate in the VPN configuration of the Securepoint Personal Firewall.

Proceed as follows in order to set up an X.509 certificate:

Call up the dialogue *VPN settings* via the menu *Advanced* and click on the folder *Key administration*.

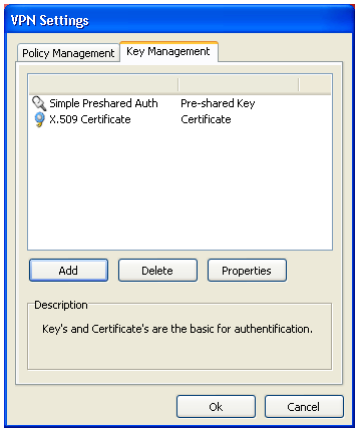


Fig. VPN settings – Key administration

- Click on *Add* and select *Certificate*. Then the certificate dialogue opens in which you can give the certificate a name and you can enter the CA identification of the actual certificate.

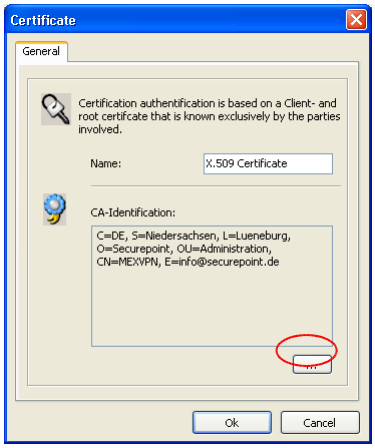
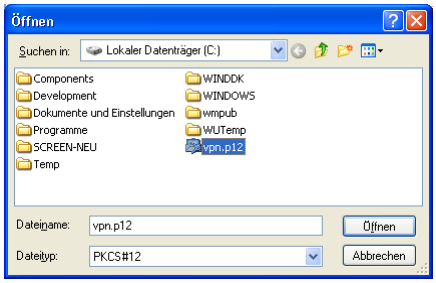


Fig. Certificate dialogue

- Open the PKCS#12 certificate by clicking on the Open button (circled above in red) and select the certificate. The certificate identification will be automatically accepted.



You can now use the set-up certificate as an authentification method in the rules administration.

5.3.4 To set up, edit and delete VPN connections

After the authentifications methods have been set up you must create a rule for the VPN tunnel which you want to set up.

To set up a tunnel connection proceed as follows:

Call up the dialog *VPN settings* via the menu *Advanced* and click on the folder *Rules administration*.

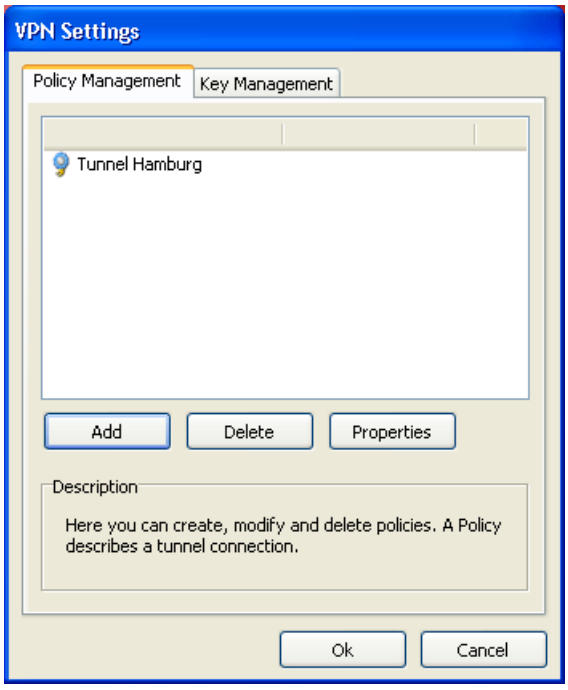


Fig. Rules administration

- Click on *Add* to set up a connection.
- Select a connection and click on *Settings* or double click on the connection in order to edit it.
- Select a connection and click on *Remove* in order to delete a connection.

5.3.4 To configure a VPN connection

To configure a tunnel proceed as follows:

➢ Call up the dialogue *VPN settings* via the menu *Advanced* and click on the folder *Rules administration*.

General Settings

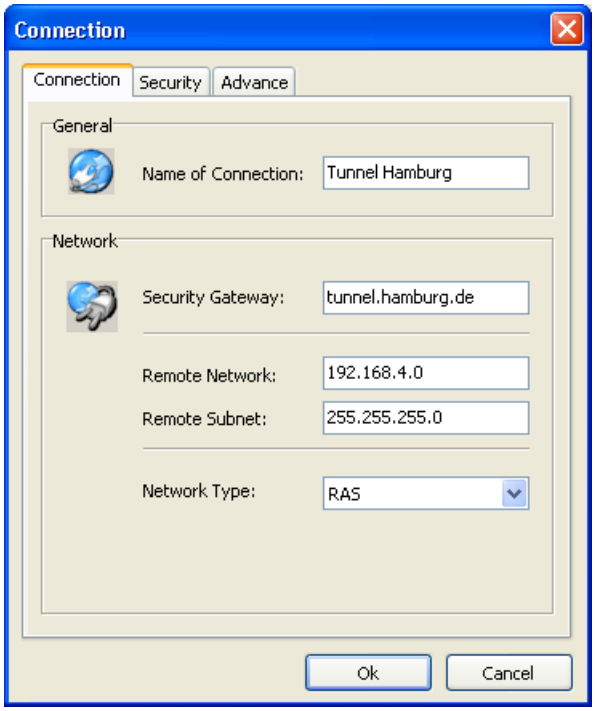


Fig. General connection settings

Description	
Name of the rule	Enter the name which identifies the connection.
Security Gateway	This is the VPN server. Enter either an IP address or a revocable Host name.
Remote network and remote subnetwork	Enter the settings of the destination network.
Network type	Indicate the type of connection to the VPN server.
RAS	The connection is set up via a dial-up connection.
LAN	The connection is set up via a LAN.
RAS+LAN	Combined status
Source and destination address	Source and destination address of the rule

Settings for the security of the connection

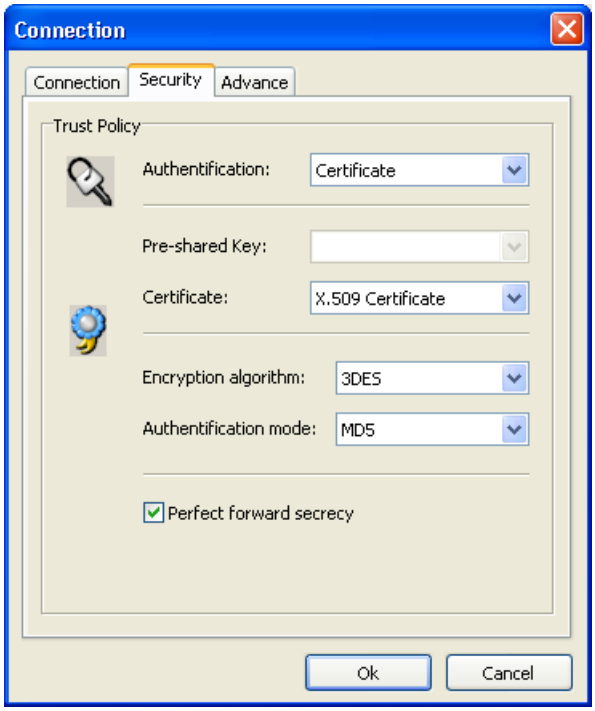


Fig. Security settings of the connection

Description	
Authentification	Enter the authentification method for the connection and select either a previously set-up pre-shared key or certificate.
Encryption	Select the encryption algorithm which you would like to use. This must be identical to the one on the VPN server.
Authentification type	Enter to which algorithm the tunnel creation should be carried out.
Perfect forward secrecy	Activates the session in PFS mode

Advanced Settings

Description	
Life cycle of the key (Re-Keying)	Indicate after which time the key should be re-generated.

5.4 A VPN with Securepoint Firewall & VPN Server and X509 authentication

o

Your aim is to connect a Securepoint Firewall & VPN server with a Securepoint Personal Firewall & VPN Client (roadwarrior) via a X509 authentication. For instance, you would like to allow a notebook to access internal resources while on the way. The roadwarrior should be able to access the internal file server via NetBios (Windows Filesharing). This should be done via a secured IPSec connection. Follow the steps to create the IPSec connection:

Proceeding in 3 steps:

5.4.1 Creating the firewall rules for IPSec connections
5.4.2 Creating X509 certificate
5.4.3 Configuring IPSec connection on the firewall

The following screens are made on the Securepoint Security Manager and nconfig program of the Securepoint Firewall & VPN Server.

o

o

5.4.1 Creating the firewall rules for IPSec connections

You would like to allow a notebook to access internal recourses while being on the way. This should be done via a secured IPSec connection.

Creating network objects

So that the external interface of the firewall can be reached by IPSec protocols (UDP/500 and ESP), you have to create the respective network objects (see Fig. Create network object fw external and Fig. Create network object fw ipsec). Thereby, control the indicated zones (sectors), also see Securepoint zone-concept.

To create the network objects, proceed as follows:

- Switch via menu Modify ⇨ Options ð Computer

or

- Open the window Rules (table) via Modify ð Rules (table).
- Click on the window's surface with right mouse key and select Computer.

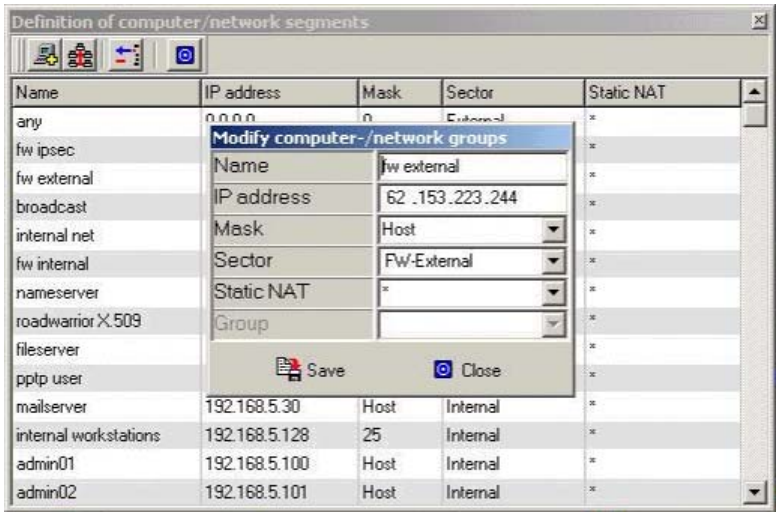


Fig. Create network object fw external

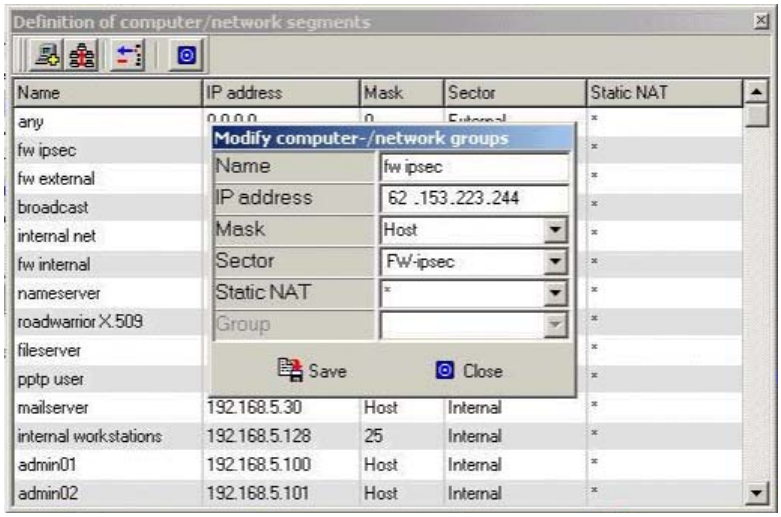


Fig. Create network object fw ipsec

Create computer group

Join the two newly created network objects in a common group.

Proceed as follows:

- First, switch via menu *Menu Modify ⇨ Options ⇨ Computer groups*

or

- Open the window *Rules (table)* via *Modify ⇨ Rules (table)*
- Click on the window's surface with the right mouse key and select *Computer groups*.
- Create the computer group Grp-fw external and add the newly created network object to the group.

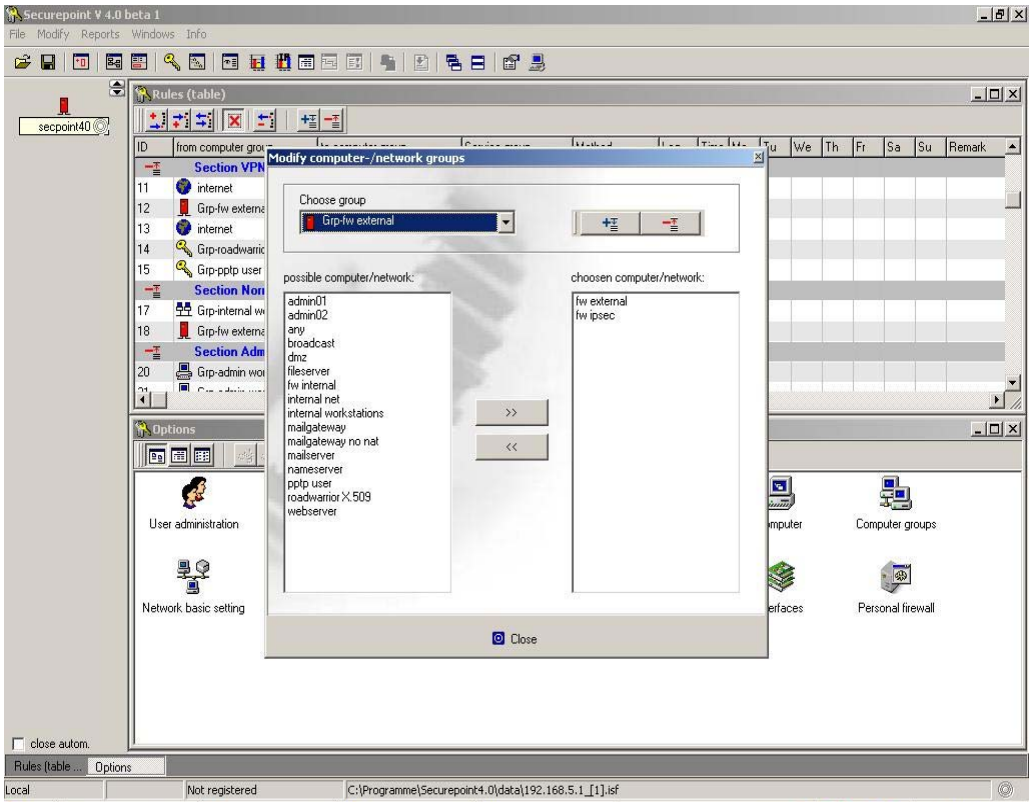


Fig. Create computer group Grp-fw external

Create firewall rules

Activate a rule with which everybody can access the external interface of the firewall from the Internet via IPSec protocol. In this case, we do not know which IP address the roadwarrior has because probably it will be given an IP address by the provider.

Proceed as follows:

➢ Switch to the window *Rules (table)* and click on the icon *New Rule*.

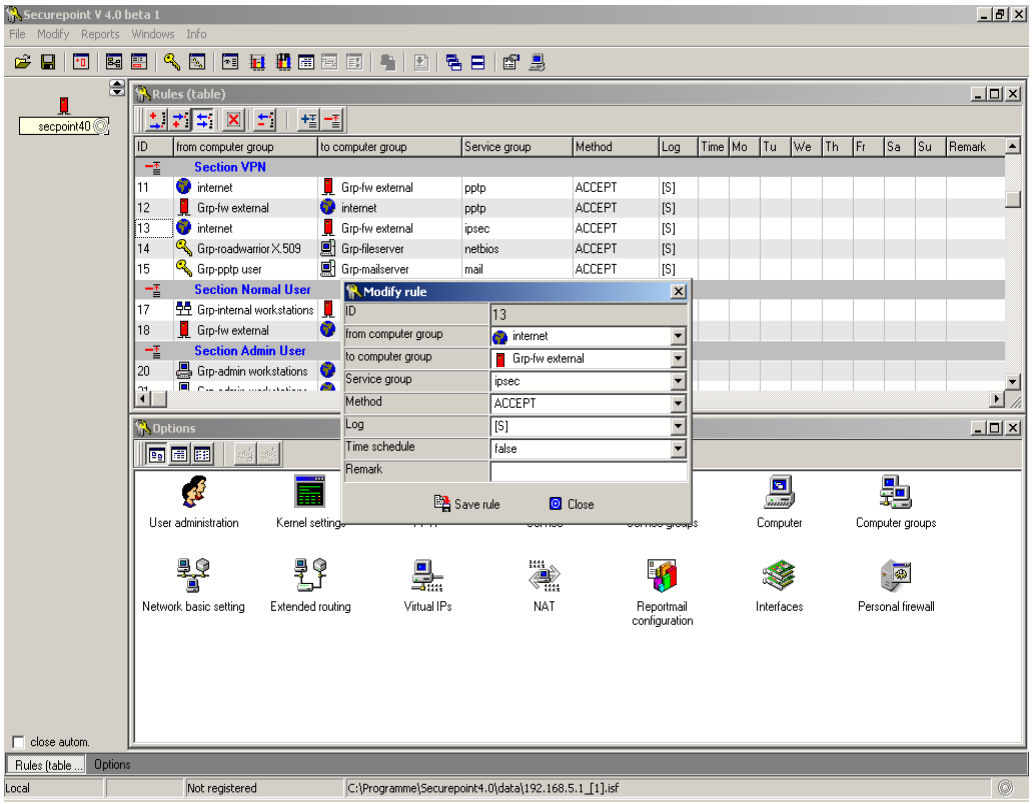


Fig. Create firewall rule

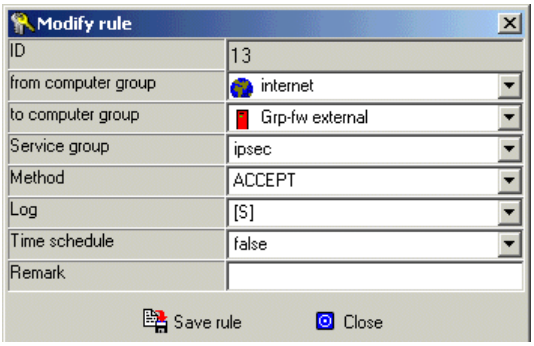


Fig. Dialog window modify rule

➢ Fill in the following data:

Fields of input and selection	
from computer group:	internet
to computer group:	Grp-fw external
Service group:	ipsec
Method:	ACCEPT
Log:	[S]
Time schedule:	false

With this rule, you allow access from the Internet on the external IPSec interface of the firewall.

Note: The service group *ipsec* is a pre-defined group which you do not have to create.

Create network objects

You have to define which resources in the internal network the authorised roadwarrior can access later on. It is proceeded on the assumption that the network objects do not exist yet. Therefore, first create the network objects for the roadwarrior and for the file server. Later on, the roadwarrior should be able to access the internal file server via NetBios (Windows Filesharing). In the IPSec tunnel, the roadwarrior has the IP address 172.16.1.10/32.

To create the network objects, proceed as follows:

- Switch to menu *Modify ⇨ Options ⇨ Computer*

or

- Open window *Rules (table)* via *Modify ⇨ Rules (table).*
- Click on the window's surface with right mouse key and select *Computer*.

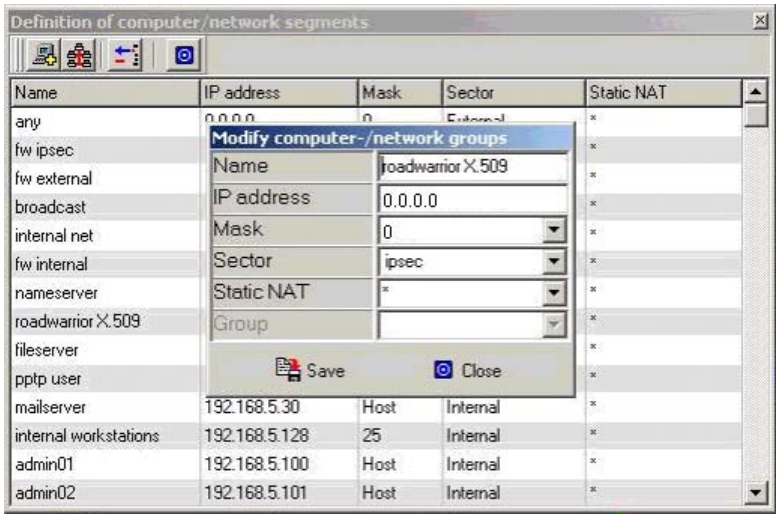


Fig. Create network object roadwarriorX.509

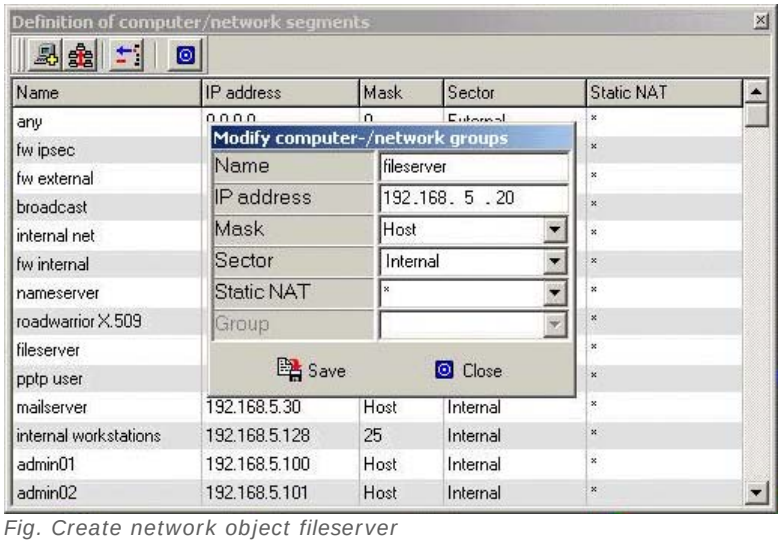


Fig. Create network object fileserver

Create computer groups

Put each of the two newly created network objects in a new group.

Proceed as follows:

- Switch to menu *Modify* ⇨ *Options* ⇨ *Computer groups*

or

- Open the window *Rules (table)* via *Modify* ⇨ *Rules (table)*.
- Click on the window's surface with the right mouse key and select *Computer groups*.
- Create the new computer group Grp-roadwarriorX.509 and the group Grp-fileserver and put each of the newly created network objects in the respective group.

Create firewall rules

Now you have to activate rules which define the resources the authorised roadwarrior is allowed to access within the internal network. In this case, it should be allowed to access the internal file server via NetBios (Windows Filesharing).

Proceed as follows:

➢ Switch to the window *Rules (table)* and click on icon *New Rule*.

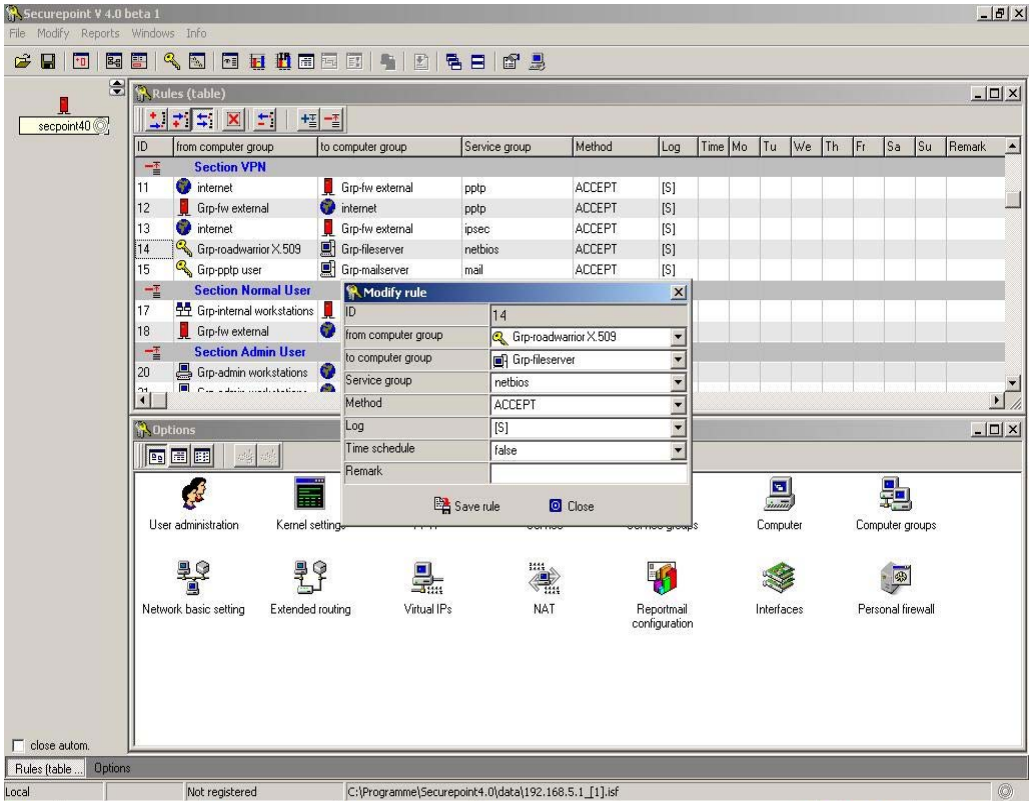


Fig. Create firewall rule

Fig. Dialog window modify rule

➢ Fill in the following data:

Fields of selection	
from computer group:	Grp-roadwarriorX.509
to computer group:	Grp-fileserver
Service group:	netbios
Method:	ACCEPT
Log:	[S]
Time schedule:	false

With this rule you allow the access from the roadwarrior to the internal file server.

Note: The service group *netbios* is a pre-defined group which you do not have to create.

5.4.2 Creating X509 certificates

Login via SSH or locally at the firewall to be able to create X509 certificates. Start the program *nconfig*. The program *nconfig* allows you to change the configuration of your firewall and to create X509 certificates.

➢ Select point: *VPN Properties.*

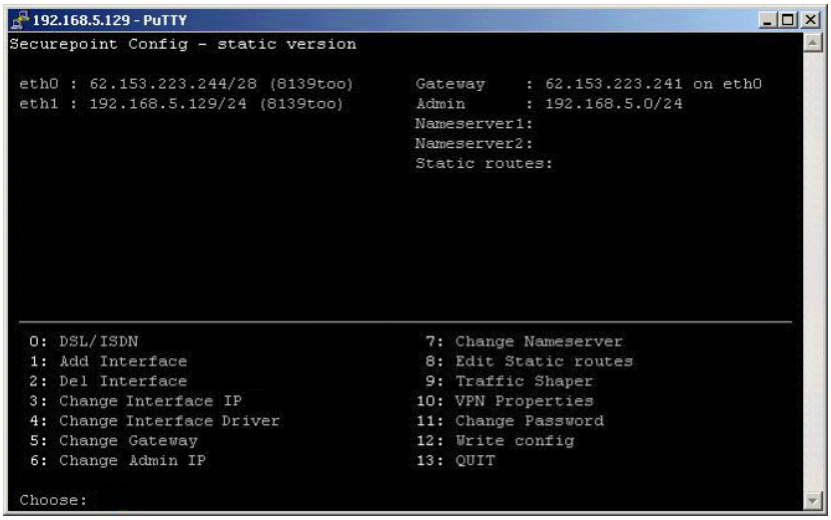


Fig. Program nconfig, selection

Creating the CA (Certification Authority)

Before you create the actual IPSec connection including X509 certificates, you have to generate the CA (Certification Authority) which will sign your certificates (Self-Signed-Certificates).

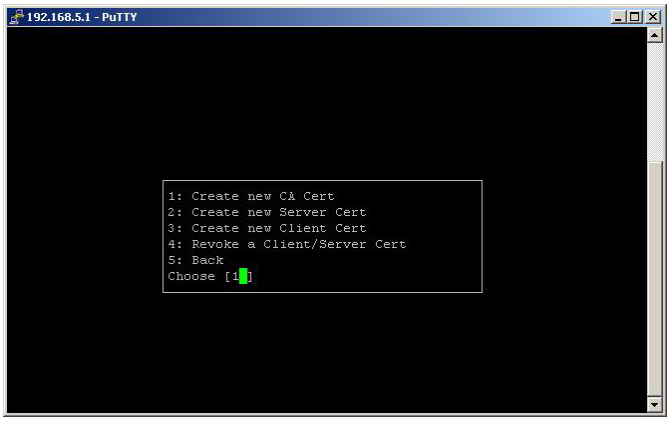


Fig. Program nconfig, create new CA cert.

- Selection: Carry out point 1: *Create new CA Cert.*

- Fill in the respective data and, what is most important, remember the password! With this password, you will be able to sign your certificates.

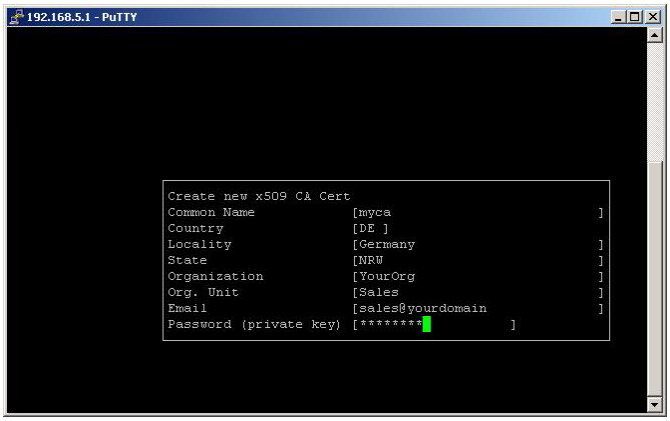


Fig. Program nconfig, insert CA data

Fill in the following data:

Common Name:	myca
Country:	DE
Locality:	Germany
State:	NRW
Organisation:	YourOrg
Org. Unit:	Sales
Email:	sales@yourdomain
Password (private key):	**********

Creating a server certificate

Now, create the new server certificate.

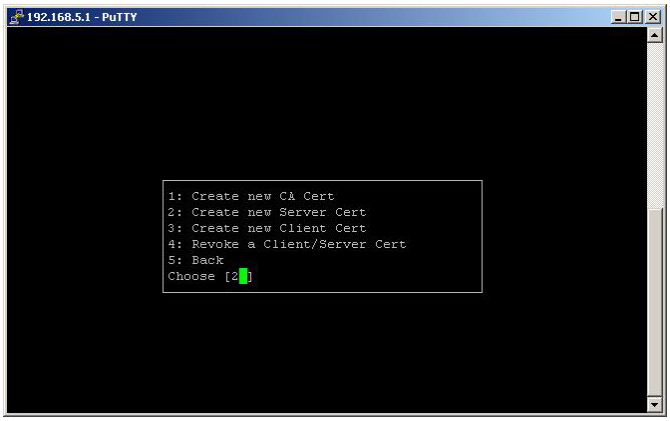


Fig. Program nconfig, create new server cert.

- Selection: Carry out point 2: Create new Server Cert.

- Fill in the respective data. You have to fill in the first password as your server certificate when creating the IPSec connection in the Security Manager. With the second password, you are able to sign your password with the local CA.

Fig. Program nconfig, insert server cert. data

Fill in the following data:

Common Name:	myServerCert
Country:	DE
Locality:	Germany
State:	NDS
Organisation:	YourOrg
Org. Unit:	Sales
Email:	sales@yourdomain
Password:	********
CA Password:	********

Creating a client certificate

Now, create the client certificate for the roadwarrior.

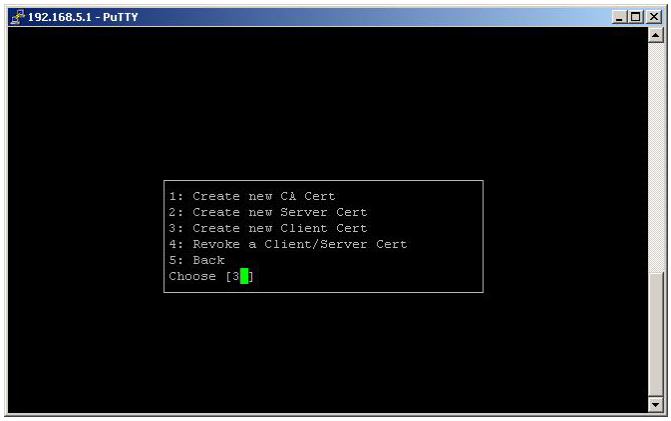


Fig. Program nconfig, create new client cert.

- Selection: Carry out point 3: Create new Client Cert.

- Fill in the respective data. You have to fill in the first password as your client certificate when creating the IPSec connection in the Security Manager. With the second password, you are able to sign your password with the local CA.

Fig. Program nconfig, insert client cert. data

Fill in the following data:

Common Name:	myServerCert
Country:	DE
Locality:	Germany
State:	NDS
Organisation:	YourOrg
Org. Unit:	Sales
Email:	sales@yourdomain
Password:	********
CA Password:	********

Exporting a certificate

➢ Now, you can export the certificate to a floppy disk or USB-stick.

The certificate will be saved under the following path on the firewall:

/opt/securepoint4.0/tmp/client_cert/

You can also download it from the firewall later on, for instance via sftp protocol.

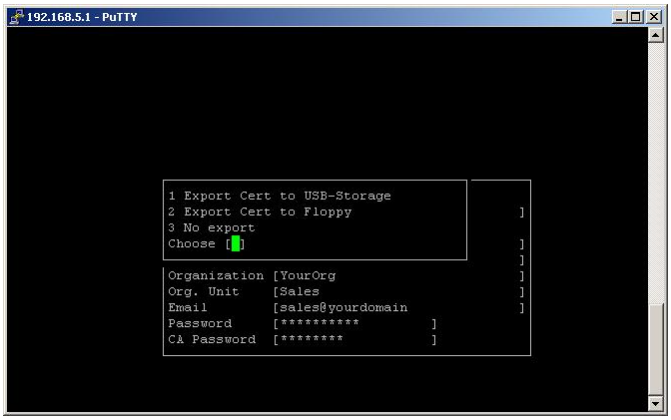


Fig. Export certificates on USB-stick or disk

5.4.3 Configuring the IPSec connection on the firewall

Now, switch back to the Security Manager (Client) and select the point *Firewalls - VPN*. To do so, open the window Firewalls - VPN via the menu *Modify* ⇨ *Firewalls - VPN* or via the icon *Firewalls - VPN*. The window Firewalls - VPN is subdivided into three parts:

- Icon bar with functions
- Firewalls – VPN list
- Worksheet (with map if desired)

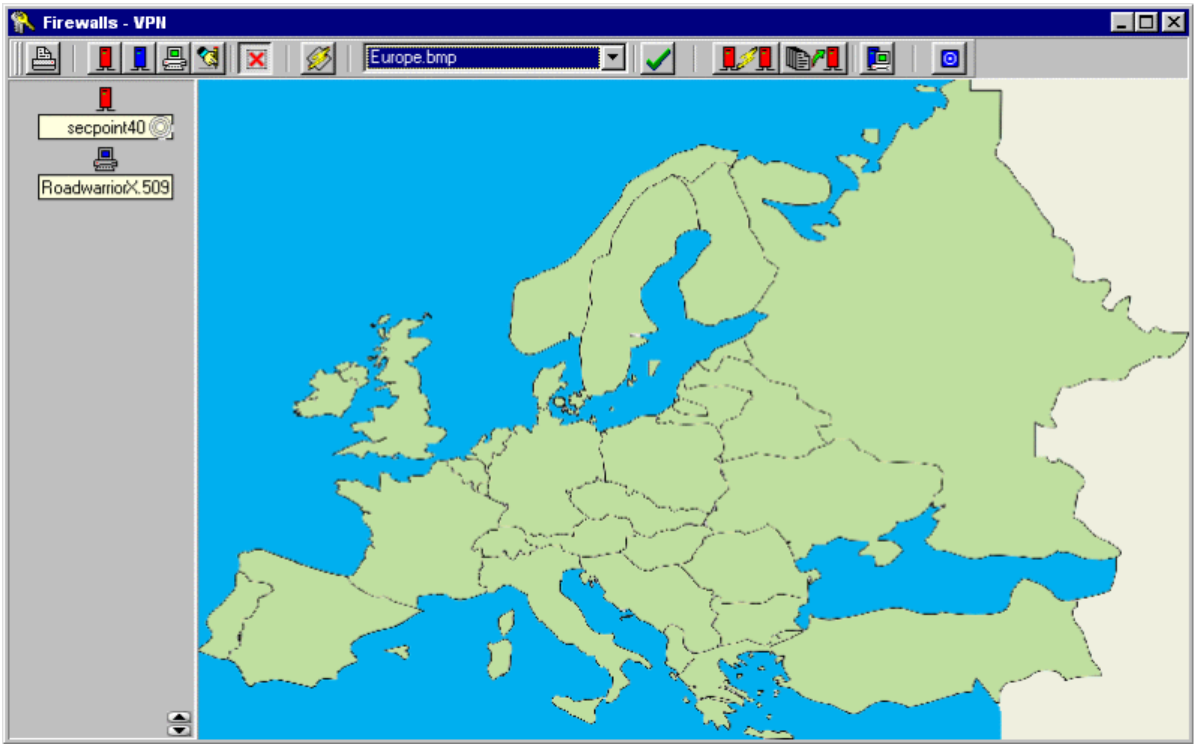


Fig. Window Firewalls - VPN

The worksheet

You have the possibility to integrate a map into the worksheet. This provides for a better overview of your VPN net. Select the map at will via the choice field (here europe.bmp). Draw the desired firewall and roadwarrior objects by drag and drop to the worksheet. In case the needed firewall and roadwarrior objects do not exist yet, create them via the icons *New Securepoint Firewall 4.X, New other firewall* and *New roadwarrior*.

Note: You can use as many maps as you like. Easy copying of the needed maps (as BMP bitmap) to the map folder of the Securepoint program makes them available for the client.

Note: You can create as many empty worksheets as you like. To do so, copy empty bitmap files to the map folder under the names like “name_at_will.bmp”. Advantage is a fast building up of the screen picture with few flickering.

Creating of a roadwarrior object

Proceed as follows:

- Select the worksheet at will (here *germany.gmp*).
- Draw the firewall object on the worksheet (*Fig. Worksheet with firewall object*).
- Create a roadwarrior object named RoadwarriorX.509.
- To do so, click on icon *New roadwarrior*.
- Since we do not know hat IP address the roadwarrior is given by the provider, fill in the IP 0.0.0.0 (*Fig. Roadwarrior object*).
- The newly created roadwarrior object now appears in the left object bar and can also be drawn on the worksheet by drag and drop.

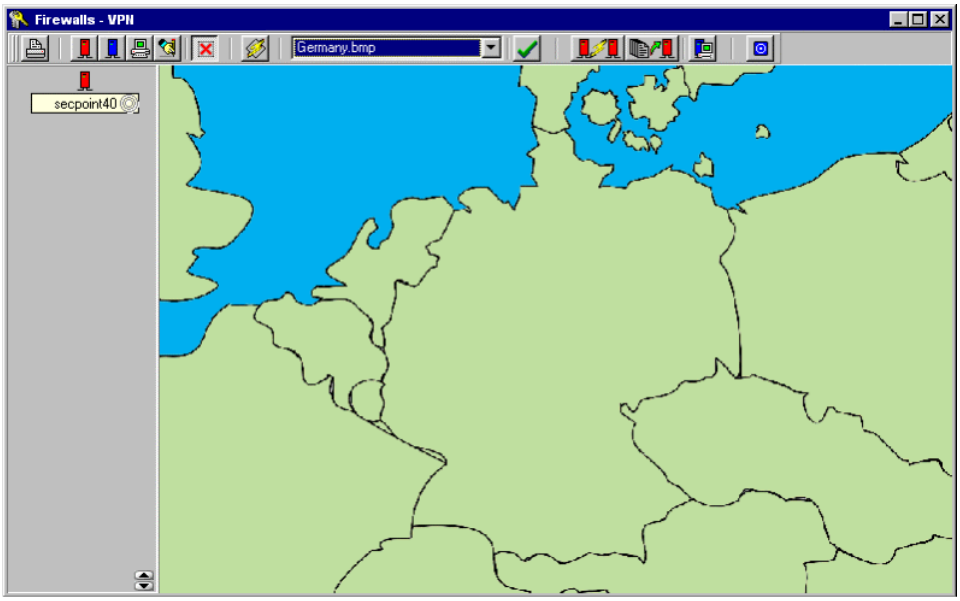


Fig. Worksheet with firewall object

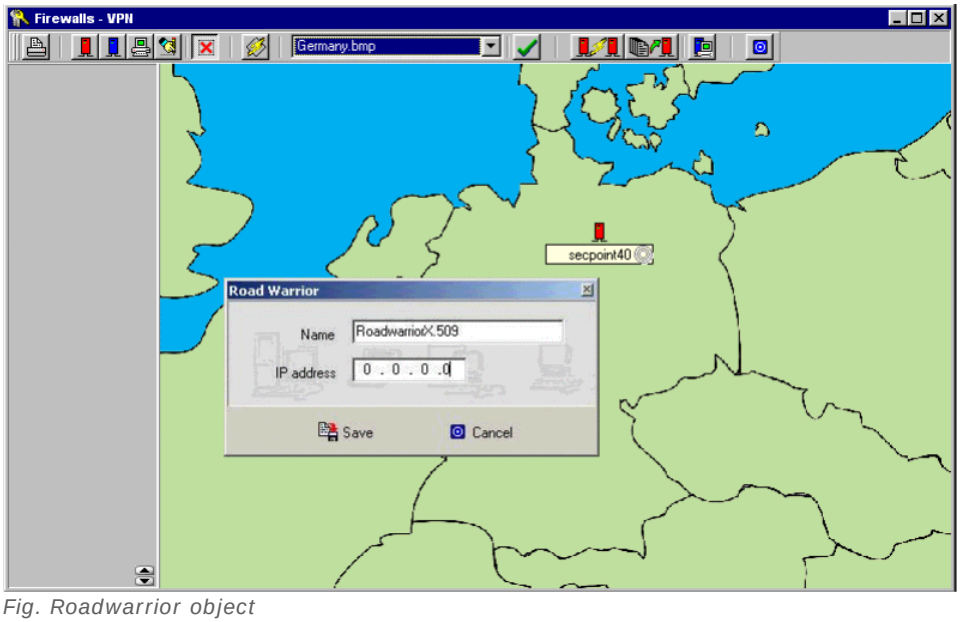


Fig. Roadwarrior object

Create IPSec connection

Now, the two objects located on the worksheet, can be connected with each other and an IPSec connection can be established.

Connect objects with each other

Proceed as follows:

- Click on the icon *New IPSec connection* in the icon list and on the firewall object.
- You receive a message which asks you to click on the targeted object – in this case the roadwarrior object (*Fig. IPSec connection*).
- The window for filling in the data for connection opens (*Fig. Dialog window properties of IPSec connections*).

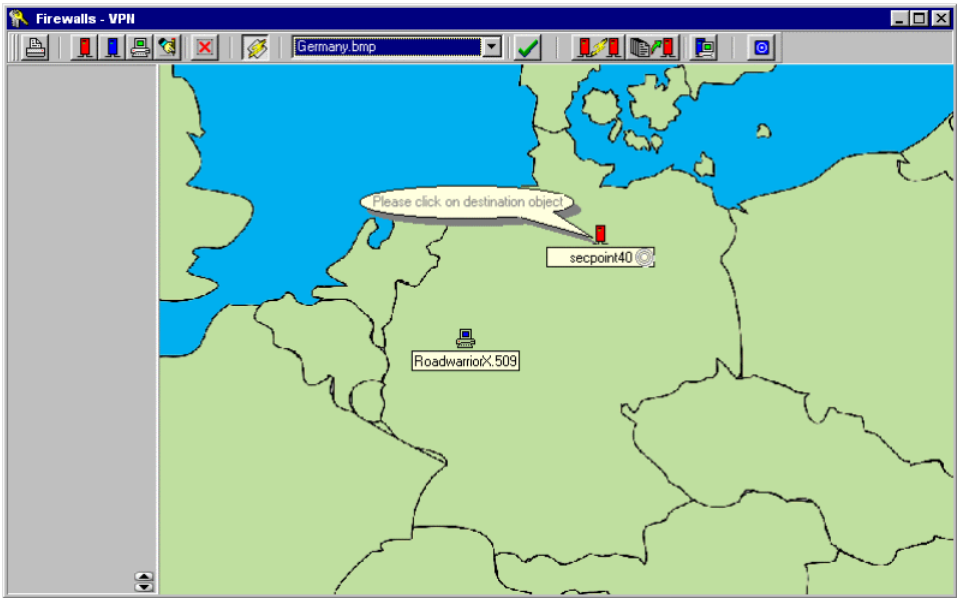


Fig. IPSec connection

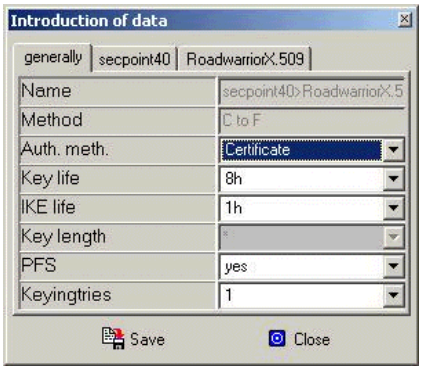


Fig. Dialog window properties of IPSec connections

Configuration of connection type

Proceed as follows:

- Now, select the type of connection and fill in the necessary data for the IPSec connection.
- Fill in *Certificate* as method of authentication in the first folder (generally).
- Switch to the next folder *secpoint4.0*. This folder has the name of firewall object.
- Select the server certificate that is to be used (Local certificate).
- Fill in the distributed password (Local key).
- Save your data.

Note: Do not fill in the CA's password to sign your certificates, but the password of the created certificate!

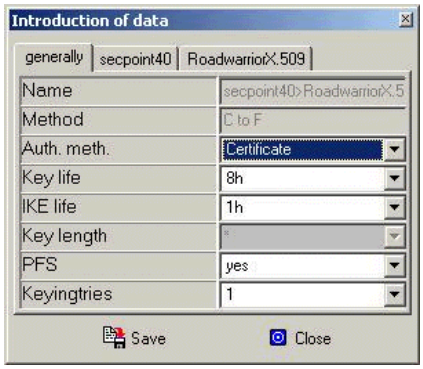


Fig. Dialog window properties of IPSec connections, generally

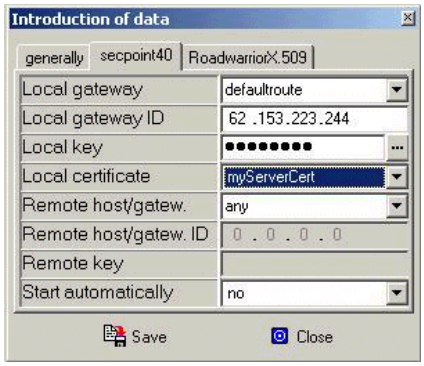


Fig. Dialog window properties of IPSec connections, secpoint4.0

Connecting nets in the IPSec tunnel

Now, fill in which nets you would like to connect in the IPSec tunnel (*Fig. Connect networks in IPSec tunnel*).

Proceed as follows:

- Click on *black rectangle* (which is located on the emerged *Linie* between firewall and roadwarrior object) with the right mouse key.
- Click on menu *Modify subnet* and fill it in.

The subnet which the roadwarrior would like to access is 192.168.5.0/24. 172.16.1.10/32 is the roadwarrior's IP address in the IPSec tunnel (*Fig. Subnet*).

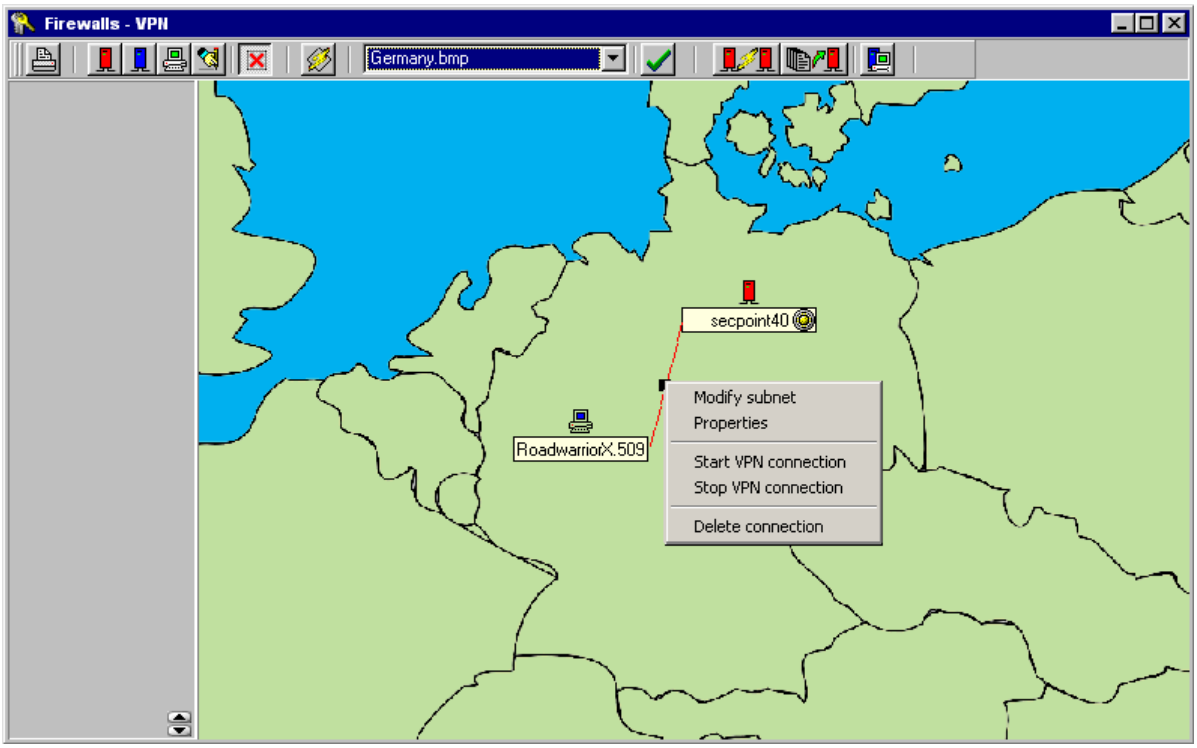


Fig. Connect networks in IPSec tunnel

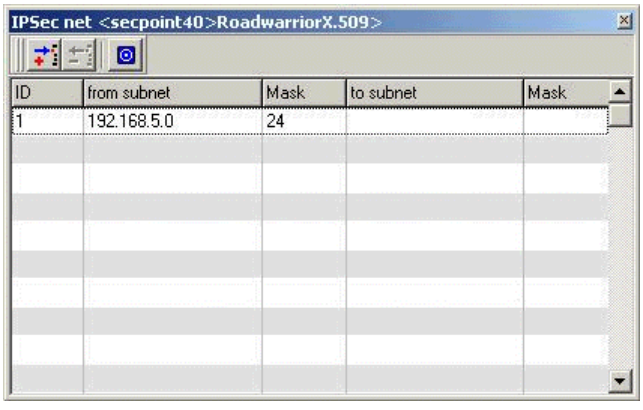


Fig. Subnet

Running the IPSec connection

If you filled in all the data correctly, the connection line will be *green*.

Restart the IPSec service on the firewall to take over the data.

Proceed as follows:

- Click on the icon with the *green hook* behind located in the icon list

or

- Click on *black rectangle* between the objects with the right mouse key
- select *Start VPN connection* from the menu.

Note: The roadwarrior wants to access the file server via the Internet. The file server's IP address is 192.168.5.20. Now, this is possible. The firewall rules are created and also the VPN configuration on the firewall is completed, the only thing that has to be done is the configuration of the roadwarrior.

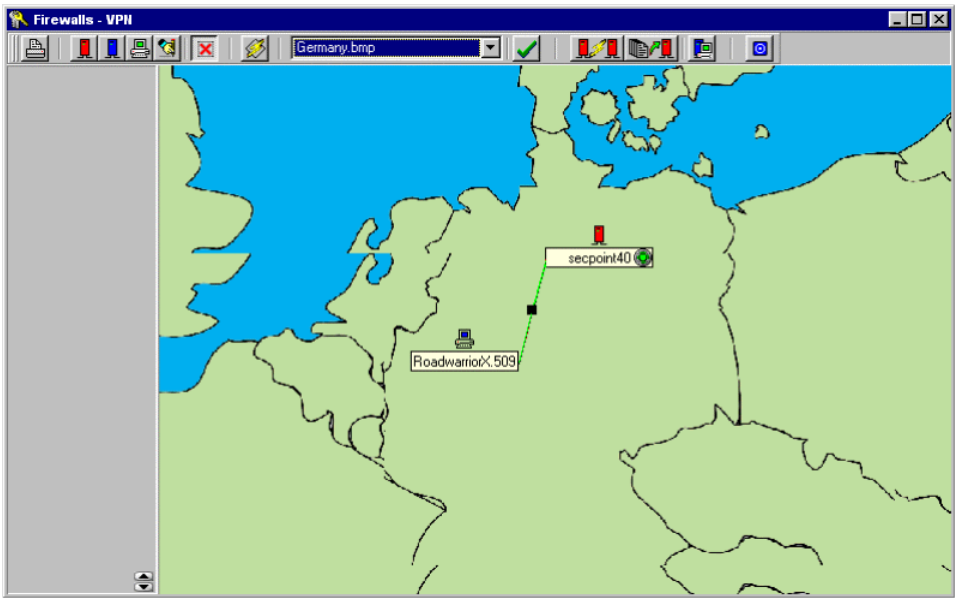


Fig. VPN connection

6 Recording and reporting with the Securepoint Personal Firewall

One of the most important functionalities of a firewall is the recording and reporting of connections. With the help of this functionality, for instance it is possible to detect attackers or get aware of other unusual activities.

6.1 Viewing record

In the overview of records (record), you can see all events such as *Erlaubte Zugriffe, Verbotene Zugriffe etc.* on your computer. Te firewall creates one record file per day which you can comfortably select via the selection window. Furthermore, you have the possibility to evaluate, save or print this data. In case any problems occur, you can draw conclusions concerning attack and attacker on the basis of this record.

➢ Call up of *Log-View* erfolgt via the menu *Events* ⇨ View *Log.*

After that, the window with the overview of records opens (*Fig. Log-View*).

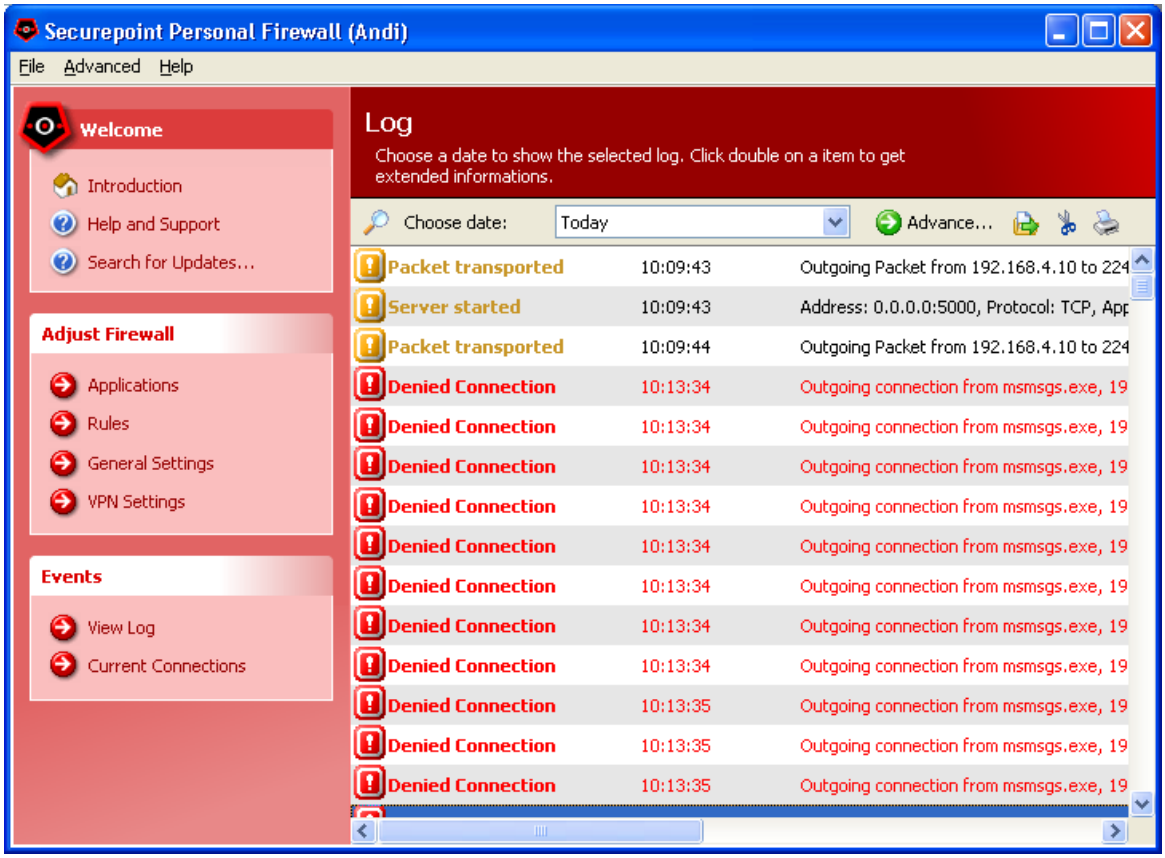

Securepoint Personal Firewall (Andi)
File Advanced Help
Welcome
Introduction
Help and Support
Search for Updates...
Adjust Firewall
Applications
Rules
General Settings
VPN Settings
Events
View Log
Current Connections
Log
Choose a date to show the selected log. Click double on a item to get extended informations.
Choose date: Today
Advance...
Packet transported 10:09:43 Outgoing Packet from 192.168.4.10 to 224
Server started 10:09:43 Address: 0.0.0.0:5000, Protocol: TCP, App
Packet transported 10:09:44 Outgoing Packet from 192.168.4.10 to 224
Denied Connection 10:13:34 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:34 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:34 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:34 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:34 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:34 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:34 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:34 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:34 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:35 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:35 Outgoing connection from msmsgs.exe, 19
Denied Connection 10:13:35 Outgoing connection from msmsgs.exe, 19

Fig. Window Log-View

Menu bar overview of records

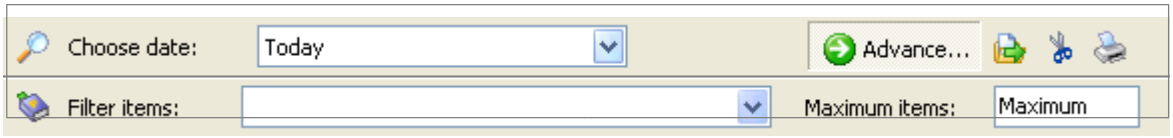


Fig. Menu bar Rules-View

Menu overview of records		
	Select date:	Selection of date filter via the choice field
Erweitert	Extended:	Opens filter settings (extended menu)
	Cut:	Current log file will be deleted
	Print:	Current log file will be printed
Extended overview of records		
	Filter entries:	Selection of filter which should be applied: - show all entries - show allowed connections only - show blocked connections only - show package notifications only - show server notifications only - show program notifications only
	Maximum:	Limitation of number of log file entries

Entry record

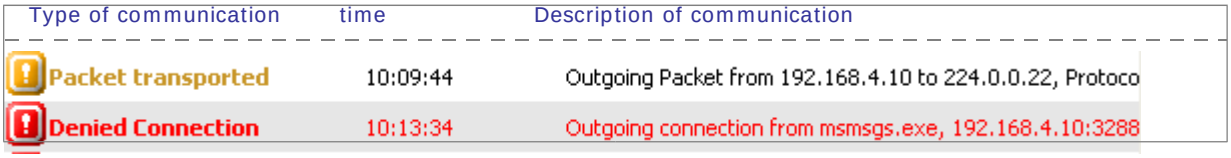


Fig. Items

Entry record	
Conducted type of communication:	Marking of the type of communication by color - allowed connections (green) - blocked connections (red) - package transported (yellow), notification of package filter - package blocked (red), notification of the package filter - server started (yellow), application works as server - notification of error in program (blue)
Time:	Time of communication
Description of the communication by:	- what application - direction, from or to your PC - address of source and target - type or record - prt

Showing entry

➢ Double click on the selected entry.

After that, the window entry opens (Fig. Window Item). Here, you have the possibility to view single log entries.

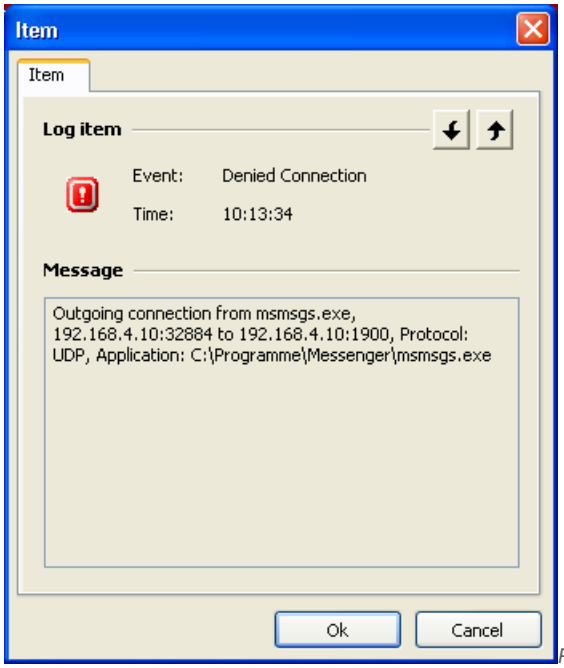


Fig. Window Item

Icons		
	One entry down:	Shows previous entry
	One entry up:	Shows following entry

6.2 Overview of statistic

In the overview of statistic, you can watch all connections arranged by applications (programs) in real time and thereby learn which interactions are currently conducted by your computer with other systems.

The overview of statistics is similar to the output of the windows command *netstat.exe*. But the overview of statistics shows you a lot more information.

➢ Call up of the overview of statistics via the menu *Events ⇨ Current Connections.*

After that, the window with the overview of statistics opens (*Fig. Statistic-View*).

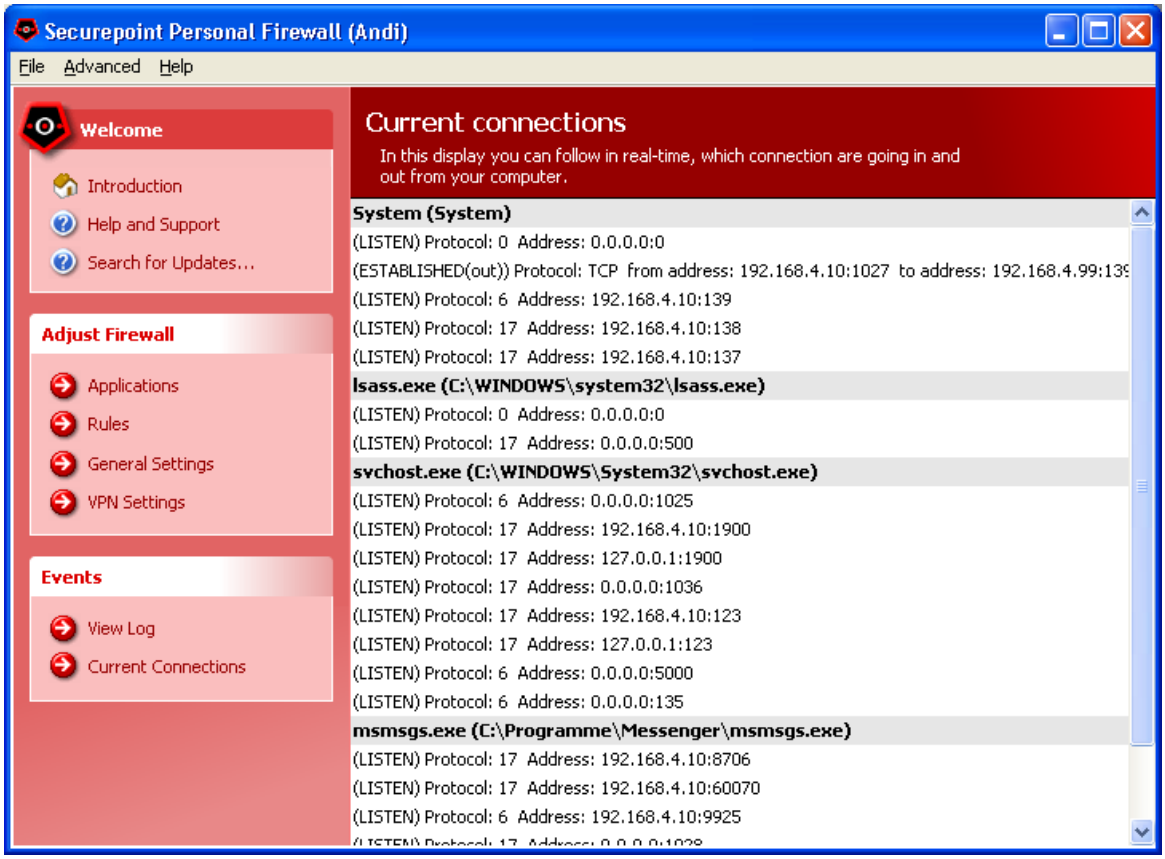


Fig. Window Statistic-View

7 Update

The Update Wizard is providing assistent to look if there is a new version available for the Securepoint Personal Firewall and automatically installs the new version.

➢ To start the Update-Wizard, click on the menu *Help* ⇨ *Search for updates.*

The update process will continue fully automatically.

Gehen Sie folgendermaßen vor:

➢ If there is a new update. Click Yes to start the installation of the update.

➢ Follow the instruction of the update process.

8 Uninstall the Securepoint Personal Firewall

Prior to uninstall the Securepoint Personal Firewall

In case the Securepoint Personal Firewall is active, you first have to end the program to be able to start with uninstalling it.

- End the Securepoint Personal Firewall.

Uninstalling the Securepoint Personal Firewall

- Clcik on the button *Start* in the windows task bar and select *Programs* ⇨ *Securepoint Personal Firewall* ⇨ *Uninstall*.

The window to delete the Securepoint Personal Firewall opens.

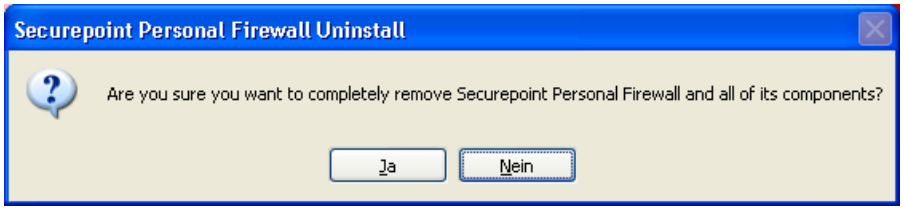

Securepoint Personal Firewall Uninstall
Are you sure you want to completely remove Securepoint Personal Firewall and all of its components?
Ja
Nein

Fig. Uninstall Wizard

- Click on the button *Yes* to proceed with uninstalling the Securepoint Personal Firewall.
- Click on the button *No* to end the process of uninstalling the Securepoint Personal Firewall.

Glossary

Applications

An application is a program which is run under the windows desktop. You can select between window applications and background applications, whereas window applications are visible for the user and whio thereby can work with the application (e.g. Word). Background applications run in the background and support the operating system in administering.

Real time services

For real time applications such as language, video or chat, there are several services available, among them talk, IRC (Internet Relay Chat) and several others.
These services allow a direct communication between users. IRC causes many scurity problems which mostly concern the used clients and servers. For instance, some clients allow servers access to local resources. The problems are comparable to those of web browsers. Therefore only use those clients that surely do not allow this.

IP addresses

By the IP addresses, a PC is clearly recognised in the internet. Your computer is automatically given an IP address when connecting to the internet. Within networks, your administrator provides for IP addresses that are given to your computer. IP addresses are necessary to send data to other computers or to receive data from other computers. IP addresses are distributed by providers and Network Information centers. This is necessary to make sure IP addresses are only distributed once. Additionally, routing is simplified.
Certain IP address areas are predestined for private usage by organisations.
These are:

Class A nets:	10.0.0.0 to 10.255.255.255
Class B nets:	172.16.0.0 to 172.31.255.255
Class C nets:	192.168.0.0 to 192.168.255.255

Those nets will not be distributed officially and should only be used for internal networks.

FTP service

The FTP service (File Transfer Protocol) serves for transferring files.
It is certainly possible that software which might be dangerous can be sent to users this way. In case you allow external users to download data from your systems, you also have to expect security problems. Usually, external users are allowed to access your FTP server via anonymous FTP. In doing so, the other users should have restricted rights. You have to configure the FTP server in this manner that external users have no access to areas that are relevant for security. Also, FTP should not be used as shell access on the system itself.

FTP problems

The classical problem with filtering FTP is that FTP has two totally different modes: the active mode and the passive mode which is also called PASV. It is standard that web browsers sign in at the passive mode. Since FTP exchange data via a control and a data channel (port 20 and 21), several problems arise. While in active mode, the server tries actively to establish a connection to the client for the data channel. The firewall can not allow this process without completely activating all ports above 1024. While in passiv mode, the client defines all channels, that is the one for control and the one for data.

Firewall rules

Firewall rules define how a firewall reacts to certain data or forms of communication. A firewall rule contains a pattern of data and an action which is to be conducted in case the pattern is recognised.

http service

The http service is one of the most frequently used services. With its help, you can receive websites on your browser. The http service (HyperText Transfer Protocol) represents a problematic service since it offers several possibilities for misuse on the client's sites as well as on the web browsers and on the server sites. Via this service, not only information but also programs can be sent. This in itself means that only by activating this service via the firewall, you create possible places where problems could arise. Additionally, gaps and errors in implementation of Javascript, Java or AktiveX programs are frequently found in the browsers. Every single program that can be run via the browser therefore represents a problem. After activating the HTTP service, you should always make sure only to load programs from the internet that were at least checked by a virus scanner and are also coming from a save address. Do not load any programs from private homepage and run them on your PC!

Mail service

One of the most popular services is the mail service. The service itself does only involve few risks. But via attachments, programs can be sent to users which have dangerous contents. Additionally, it is quite easy to forge emails. For instance this was one reason why the virus of ILOVEYOU-Virus was so successful. It read email addresses from address books of weakly protected mail clients and sent itself to those addresses. The recipients opened the emails in many cases since they came from a familiar address.

Name service / DNS

The name service and DNS-Dienst translate IP addresses into PC names and vice versa. For instance the address: http://www.securepoint.de <-> 62.116.166.60
This service makes sense because you do not have to fuill in an IP address in case you want to access a web server. The risk in offering DNS is that you reveal information about your PC.

Net masks

The net mask is responsible for the size of your net. Net masks can also be given in bitcount.

Examples for net masks

Net	*Net mask*	*Net mask bitcount*
Entire net:	0.0.0.0	⇨ 0
Class A net:	255.0.0.0	⇨ 8
Class B net:	255.255.0.0	⇨ 16
Class C net:	255.255.255.0	⇨ 24
One PC: 255.255.255.255		⇨ 32 (Host)

protocol

A protocol is a connection language between two computers. Protocols are rules which control communication and data transfer between computers. Examples are HTTP, FTP, SMTP.

Proxy

A proxy is a computer or program which protects data traffic between computers or networks from attacks from the outside.

Server

A server is a computer or program which has central tasks within the network. A mail srvere, for instance, is responsible for sending and receiving electronic mail.

SMTP

The Simple Mail Transfer Protocol (SMTP) is the internet standard for sending and receiving emails. The protocol itself does not represent a problem concerning security, but it is not like this with SMPT servers. Here, log-ins and passwords are transferred which can be caught. Some mail servers can be misused for spam mails due to an insufficient protection and thereby masses of mails can cause the loss even of a powerful server.

TCP/IP

These abbreviations stand for Transmission Control Protocol/Internet-Protocol. TCP/IP are technical transmission protocols of the internet.

telnet service

The telnet service allows users to use a distant system. The telnet service is a very insecure service because all sent information is not encoded. Therefore, it is possible to overhear this service.

Besides telnet, there are other services such as rlogin, rsh and on. The require a surrounding of reliable PCs. Bur reliable PCs are not to be found on the internet since you should not trust any PC outside of your network. You can never be sure where the received data packages really originate from.

Trojans

Trojans are harm-doing programs which are hidden in a so-thought useful program.

Virus

A virus is a small little program or program code which accesses the computer without the user noticing it. The virus takes influence on the computer against the user's will. Most viruses are transmitted via the internet or mail programs such as Microsoft Outlook. They use the respective address book for mass spreading. Most viruses are caught by up to date anti virus programs.

General questions and answers concerning security

Why do I need a firewall?

You read more and more often about security problems in newspapers, journals and even on the internet. Where does that come from? In every society, you find individuals that are not obeying the rules. Nowadays, you find an increasing number of internet users, either in companies or in the private sector. A little share of these users is interested in finding security gaps and to use them for his purposes. The reasons for that range from childish interest and hunger for knowledge to intended sabotage.

Due to the numerous possibilities of distributing informatuion and applications on the internet, also inexperienced users quickly find themselves in a position which allows them to spy out information and conduct attacks. If you apply common statistics on criminal energy in our society to the internet community, it would be several millions of people. And why should internet users behave essentially different than in every day's life?

The more important and sensitive your data is, the more you have to protect it. Just like you have at least one lock at your door, you should have a firewall.

What is to be protected?

The first thing you have to consider is what data should be protected when connecting to the internet or to another net.

Basically, you should protect the following:

- Data and software, this is your programs and information on your PC
- Hardware, this is your PC on which the applications run and data is transported
- and yourself: self-protection

Daten- und Software

One of the most important areas that has to be protected on your PC is your data. Ponder yourself what would happen in case all or part of your data is lost, changed, or laid open to others. At least cost would have to be paid for repairing your data. In the worst case it would have consequences concerning your existence.

Therefore, you have to protect your data in concern of the following aspects:

- concerning availability
- concerning integrity
- concerning reliability

Also note that the mentioned problems with data are sometimes not immediately noticed. In many cases, the problem occurs after a longer period of time and thereby the damage is even bigger. It is easier to react to a just occurred and obvious than to a difficult manipulation which in many cases can also not be traced back to its source.

All programs on a PC, from operating system, hard disk, office applications to mail programs, are used to control, change and administer data. In many cases, these applications have possible areas where problems could arise because via these programs, other programs can be started by which things can be deleted or data can be changed. The data transfer of these programs can be overheard and for instance be checked for passwords or things like that.

It is also sometimes possible to channel programs into your programs which behave like a spy or saboteur. The more important and the more often you uses such programs, the more dangerous become these problems.

You have to protect your software concerning:

- Insight in data
- Manipulation of your data or programs

Hardware

Also the hardware should be protected. Open accesses to your PC via a router, a modem or a ISDN card represent potential danger. Also the resources of your computer should be protected against unlicensed access. Because they are a possible means to use PC time, telephone connections and a lot more without you getting to know it. Thereby additional costs can occur which you will have to pay or you might not have the complete access to your resources any more.

Therefore, you have to protect your hardware concerning:

- Access
- Resources

Self protection

Even if you have met the above mentioned requirements, it does not mean you can feel 100% save. It is for sure that you can feel a lot saver now than before. But you should also observe certain rules. For instance, you should keep password to yourself, chnge them regularly, and software should not be downloaded from the internet and started on your computer. Therefore, inform for instance your family.

Against what should I protect myself?

To protect one's self effectively, you first have to realize against what the protection should be. Since a recognised problem is easier to handle than an unrecognised one. Your PC can be attacked in many ways. The ways of attacking can be categorised.

Systemlahmlegung One of the most common problems is the complete knock out of a system. In case a service does not work properly any more, this has in most cases effects on the whole system. You surely remember the ILOVEYOU virus. Other damages concerned for instance Yahoo. The search engine was not available for hours.

Datendiebstahl Another common manes – with often far-reaching consequences – is the theft of data. Preferred data is log-ins and passwords because with them, you can conduct further actions. As soon as an attacker has got to know the log-in and password combination, he is able to do everything to which only the actual user would be allowed.

Systemeinbrüche In case of someone braking in your system, an attacker wants to use your resources, that is your applications and data, for further actions. Breaking ins in your system can be done by programs that were channelled into it, for instance by hidden programs in email attachments or in downloaded programs. In this case, programs are run in the background of the PCs which allow manipulation and also conduct them, without the user getting to know it. For instance back office is such a program with which a whole system can get under control of an attacker.

What possibilities do attackers have to find out information?

There exist several common possibilities to do so. Just to name a few:

Zufällige Anfrage A common variety is finding out information by application by chance. Many people use easy combinations for log-ins and passwords which are easy to remember. In case an attacker knows the person and his surrounding, it is very likely he also knows the relevat information.

Listen Another variety is conducted via lists of log-ins and passwords. Those lists are available on the internet, combined with the respective programs. They were created on data taken from statistics on users' behavior. The programs try to find out log-ins and passwords by filling in the data of the lists until they are successful or not.

Sniffen A method which is a bit more complicated is the sniffing of information. Via so-called sniffers, mostly log-ins and passwords are spied out. To do so, the traffic of data between applications is examined and filtered for this information. Unfortunately, this information is sent at the beginning of communication and not is encoded in the case of many programs. With a bit of patience, it is possible to find out the desired information by using this method.

DoS Attacks The attacker currently sends packages with wrong TCP check sums.

Spoofing IP addresses are pretended by spoofing. In this case, an attacker breaks in the communication between two users. The following example makes understanding easy: PC C, the attacker, overhears the data traffic between PC A and PC B. In case PC C wants to break in PCA, it first has to knock out PC B. To do so, it constantly asks PC B to build up a connection with it. But it never signs those requirements. Thereby, PC B is too busy to keep up the communication with PC A. PC C now has the possibility to pretend to be PC B and to break in PC A. By doing so, it exactly behaves like PC B.

Ping of Death This attack is based on way too large ICMP packages.

(Fragment Bomben) Teardrop and Bonk are attacks that are mainly aimed at WindowsTM servers. They are based on overlapping fragments. To avoid those attacks, all fragments have to be blocked or a reassembling has to be conducted within the IP stack.

Back Orifice Back Orifice is a program which was created by the group Cult of the dead cow Communications. This program allows you to control the PC of a user whom you actually do not know. This can be done via a usual network or via the internet. Back Orifice installs itself and allows an attacker to have complete control over a whole system.

Weitere

– Aimspy
– HackersParadise
– Doly Trojan
– SatanzBackdoor
– Sync Scan
– Fin Scan
– Barb wire, etc.

c) How can I protect myself?

There exist several methods to protect one's self. There is at least that security which is provided for by the producer of the system. But that is not enough

Few communication The first measure to provide for protection is to reduce communication. Less communications means fewer points of possible attacks. The extreme scenario would be that a totally isolated system is the safest system. Since this does not make sense regarding the numerous advantages of communication, only those services should be available that are actually needed.

Using firewall

The Securepoint Personal Firewall will protect your PC from unwanted attacks from the outside and thereby protect your personal data. Nowadays, the most common field of usage is the protection against attacks from the internet. The Securepoint Personal Firewall represents the connection between your local PC and the internet. It supervises all data traffic. The personal firewall hides your PC automatically when being online. That means it makes your PC invisibe for possible attackers. It also catches suspicious connections. Passing on personal data vuia the internet without noticing it is avoided.

The Personal Firewall of SecurepointTM suits for protecting from and supervising of e.g. TCP/IP attacks. It provides protection against attacks on the TCP/IP stack and protects from SYN flooding attacks and a lot more.

What do I need the protocols and statistics for which are provided by the firewall?

Basically no attacker would like to be identified. Many attackers and especially the greenhorns among them, are not successful in their intentions. Because of this, it is important that attacks are recognised and the conducted actions are logged to be able to identify an attacker by tracing back. That means besides protection it is also important to record incidents. This is one main feature of the firewall.
Log files should be regularly adjusted to have the best chances to detect an attacker. Every attacker wishes to delete entries in log files as soon as possible to remain undetected. The recording function includes a protection against being flooded by thousands of identical entries. But there still exists no protection against sent attacks with changing method of attacking.

Questions and answers to the Securepoint Personal Firewall

Registration

Why do I have to register the firewall?

To be able to use the firewall completely and without restrictions, you have to register for it. Thereby you get the possibility to use free email support and updates.

I receive the notification that I am already registered and the firewall ends itself automatically?

You tried to install the firewall two times on the same PC. Please contact Securepoint so that we can delete the registration from our data bank. Please note that we can only do this during the testing time.

I have made a mistakes when typing in the data?

Please contact Securepoint giving your registration key and the changes.

My license key does not work?

Fill in the exact license key in the respective field (see chapter 2.2.2). Please contact Securepoint with your registration data in case you have furthermore problems with your license key.

Where can I buy the firewall?

Click in menu *Hilfe* -> on *Registrieren* to start the contract of sale (also see chapter 2.2.2).

Basic configurations

What steps does the firewall take in case of an attack?

The firewall first filters every package before it can cause any damage at the firewall itself. The firewall operates on the Kernel level, that means in the deepest layer of your PC. The packages will be examined according to the filter rules and according to the result, they will be forwarded or blocked.

What is the basic configuration of the Securepoint Personal Firewall?

The basic configuration of the Securepoint Personal Firewall is: Without permission, everything is forbidden. This means that only applications whose communication you have explicitly allowed, are let through by the firewall.

Are there any ports open although I did not activate them?

No. Without explicit permission, all ports are blocked.

Why can I not avoid that the firewall starts automatically?

After installing the firewall, it is a part of the operating system and ue to that fact always started when the operating system is started.

Why does my Windows XP Desktop stand still when I re-register?

The computer has not broken down. Press CTRG+ALT+Del to get back to the desktop.

Which protocols are allowed by the firewall?

All protocols IP protocols that are registered at IANA (http://www.iana.org) as well as the ICMP protocol are accepted.

Can I also use the firewall under Windows 95/98 or ME ?

No, the firewall was only developed for versions of windows 2000 and higher.

Application and rules

My browser "Internet Explorer" says "The site for search could not be opened"?

Please make sure that the internet explorer was activated as application or that a respective firewall rule exists.

My computer does not allow any communication and does not demand in case I try to go online with an application?

Have you activated the emergency-off function? Please de-activate the emergency-off function to get back to normal working mode.

How can I block applications so that they do not have access to the internet anymore?

Set the selected application to mode "avoided". Further information in chapter 5.2.2.2.

Why can I not transfer data to the internet by my application?

Either activate the application via the overview of applications (chapter 5.2) or you will be asked by the demand assistant if you would like to allow the procedure or block it.

My FTP program can not connect to my server anymore?

Set the FTP connecting mode to passive.

The activation of windows network does not work anymore?

Activate the *Expertenmodus* and add the two rules "Windows file and printer activation" and "Windows ntwork activation" in the category "network rules" from the library of rules.

No further applications should be recognised. What can I do?

Activate the check box "no recognising of applications" to be found in general settings (see chapter 5.1).

How is the interdependence of firewall rule and application rules regulated?

Firewall rules have a higher priority than application rules.

Can I export my rules to the experts' mode?

Only if you have created them with the help of the library.

What happens if I do not allow svchost.exe to access the internet?

svchost.exe is the main service for communication between windows and internet or network. You have to activate this application. Remark: under windows 2000, the file is named service.exe.

Can I de-activate the application mode (silent mode)?

Yes, activate the check box under *Allgemeine Einstellungen* -> folder *Erweitert* -> "no recognising of applications".

The resources of my system are exhausted since I installed the firewall. What can I do?

De-activate and extend the time of carrying out the applications' protection under *Allgemeine Einstellungen* -> folder *Erweitert*.

How can I prevent being pinged?

It is standard that all messages via ICMP protocol are blocked

What can I do to avoid other computers pinging me?

Add the two standard ICMP messages (Echo, Echo Reply) from the library to your set of firewall rules.

How can I block a single internet address (e.g. sex.de)?

Define a new TCP rule with the setting targeted address "sex.de" and Port "80". Further information on creating rules in chapter 5.2.3.1.

Can I protect my settings from access by unauthorised people?

Yes. You can protect your settings by a password. You can define your password in the settings of the firewall (chapter 5.1).

Why does loading the record take so much time?

He larger a file is, the longer it takes to load it. You can avoid this by selecting a filter setting under the setting “extended” prior to selecting the respective log file.

Why is my game interrupted by the firewall?

Activate the application prior to starting the game.

Support

When can I get help?

You receive further help to the Securepoint Personal Firewall in the online forum under: http://www.pcschutz.de/forum/